EU AI Act Compliance Guide

Publisher: SimpleAct · https://simpleact.de
Version: 1.0
Contact: info@simpleact.de · support@simpleact.de
As of: March 2026 · Not legal advice

Legal notice

This document does not replace legal review. It maps common EU AI Act terms and obligations for **organizations that deploy or place AI systems on the market**. For binding assessments, involve your legal and compliance teams.

Keywords: EU AI Act, EU AI regulation, AI compliance, high-risk AI, AI documentation, conformity assessment, deployer, provider, GPAI

Core problem and the SimpleAct framework

Core problem

Teams often lack a **continuous chain** from transparency to evidence under the EU AI Act:

- **Obligations** are discussed, but **inventory**, **risk class**, and **roles** are not consistently documented.
- **Technical documentation** sits across inboxes, drives, and tickets - with **no shared schema**.
- **Changes** to models, data flows, or interfaces are hard to **reconstruct** for audits and leadership.
- **Tool silos** (DMS, ticketing) store files but do **not** replace a unified compliance model.

The SimpleAct framework

SimpleAct is the **AI Act compliance platform** built around a **shared five-phase reference model** across all materials:

Phase	Organizational focus	What SimpleAct brings together
1. Inventory	Transparency for systems, vendors, and data flows	A **central register** with consistent required fields
2. Risk & roles	Risk classes, deployer / provider, supply chain	**Guided classification** with documented decisions

3. Documentation	Annex IV, Art. 11, and related obligations	**Structured templates** instead of ad hoc files
4. Evidence & export	Defensible history; reports for legal, leadership, partners	**Unified exports** and traceable change records
5. Audit readiness	Updates when models, data, or products change	An **end-to-end chain** instead of folder and ticket silos

Note: This framework is the **same shared reference** in every SimpleAct document - guides, checklists, inventory, and documentation templates align to it.

---

1. What the EU AI Act regulates

Regulation (EU) 2024/1689 establishes binding rules for **AI systems** in the Union, aiming to protect health, safety, and fundamental rights while supporting the internal market.

Term	Short meaning
AI system	A system using machine learning and/or logic-based approaches; obligations depend on risk class and role.
Provider	Develops an AI system or has it developed and places it on the market under its own name/trademark.
Deployer	Uses an AI system under its authority (except non-professional/private use).
Importer / distributor	Supply-chain roles with specific duties depending on context.
High-risk AI	Systems listed in **Annex III** that meet the relevant criteria (and do not fall under exceptions).
Conformity assessment	Process demonstrating compliance with applicable obligations.
Technical documentation	Evidence package, especially for high-risk AI (including **Annex IV** structure).
Post-market monitoring	Ongoing monitoring after placing on the market / putting into service.
GPAI	General-purpose AI models with dedicated transparency and (where applicable) systemic-risk logic.

---

2. Risk ladder and obligation logic

The AI Act uses **risk categories**. Operational work requires: **which category** applies and **which role** your organization plays.

Unacceptable risk

Certain practices are **prohibited** (e.g., depending on design: certain **social scoring** constructs, certain **remote biometric identification** in publicly accessible spaces, subject to legal conditions). This is not "minor non-compliance" - it is **do not deploy** in the prohibited form.

High-risk AI

High-risk applies where **Annex III** use cases are relevant **and** the high-risk criteria are met. Typical obligations include:

- **Risk management system**
- **Data and data governance** (where applicable)
- **Technical documentation** (including **Annex IV**)
- **Logging** (where required)
- **Transparency** and **human oversight** (where required)
- **Conformity assessment** and **EU declaration of conformity** (where applicable)
- **Post-market monitoring** and **serious incident** processes

Keyword focus: high-risk AI, Annex III, Annex IV, technical documentation, EU declaration of conformity, deployer obligations.

Limited risk

Primarily **transparency** obligations (e.g., informing users, labeling AI-generated content - subject to legal interpretation).

Minimal risk

Few or no specific obligations; voluntary transparency still helps governance.

---

3. Roles: provider, deployer, supply chain

Provider

Often responsible for **technical documentation**, **conformity processes**, **CE marking** (where product law applies), **quality management**, and **incident** pathways - depending on product and risk class.

Deployer

Must ensure **appropriate human oversight**, **input control**, **logging** (where required), **incident handling**, and updates for **substantial modifications**. **Purchased AI** still matters: you may be deployer even if you do not train models.

Importers and distributors

Verify **documentation**, **labeling**, and **handoff** to downstream actors - align procurement and legal.

---

4. Technical documentation and conformity

For **high-risk AI**, **technical documentation** is the core evidence. It typically covers:

- System description, intended purpose, **intended users**, and **limitations**
- **Validation** and testing strategy
- **Data** (training/testing where relevant)
- **Risk management** and post-market processes
- **Cybersecurity** and lifecycle management

Annex IV provides a structuring framework for documentation content.

Conformity assessment may be internal, notified body involvement, or hybrid - depends on product context.

---

5. GPAI and transparency

GPAI models may trigger **transparency** and **documentation** duties depending on whether you are an upstream model provider or a downstream system provider. For SaaS vendors, the chain **base model -> product features -> tenant configuration** determines responsibility splits.

Keywords: GPAI, general-purpose AI, downstream documentation, licensing.

---

6. Timelines and transition

The regulation introduces **staggered applicability** (prohibitions, GPAI rules, high-risk obligations, product-related links). Run internal **roadmaps** and maintain a **central AI inventory** so deadlines and evidence are managed together.

---

7. How SimpleAct helps: The AI Act Compliance Platform

SimpleAct is not "just another single-purpose app." It is an **AI Act Compliance Platform**: a continuous workflow from **AI inventory** and **risk classification** through **structured documentation** and **tamper-evident evidence** to **exportable audit reports**.

Why "platform" vs "tool"?

- **End-to-end:** One system for **all** relevant AI assets per tenant, instead of spreadsheets, tickets, and email threads.
- **Compliance-by-design: Mandatory fields**, **risk questionnaires**, and **evidence** are structured - not optional attachments.
- **Audit readiness: Exports** (PDF/DOCX) and **traceable changes** support audits and oversight conversations.
- **Roles & accountability:** Ownership and approvals align with governance expectations.

Contrast with generic software

- **Ticketing tools** track tickets, not **risk class** or **Annex IV** documentation.
- **DMS** stores files, not structured **AI system metadata** with compliance versioning.
- **ML platforms** focus on training/deployment, not regulatory **evidence chains**.

Coverage map

Area	Value
AI inventory	Full capture including **shadow AI** risk; **keywords:** AI register, AI asset inventory.
Risk classification	Guided mapping to EU categories with **Annex III** awareness.
Documentation	Structure for **technical documentation** and operational evidence.
Exports & reports	Evidence packs for **audit**, management, and external reviewers.
Traceability	Changes are traceable - not "the PDF from last week."

Pricing: From €199/month (see website for current plans).

---

8. Glossary (selection)

Term	Explanation
FRIA	Fundamental rights impact assessment (where applicable).

Notified body	Conformity assessment by accredited body (where required).
CE marking	Where product law applies.
Logging	Event records for traceability and oversight.
Human oversight	Human control and intervention capabilities.

---

9. Practical checklist and common mistakes

Checklist (extract):

1. Is every AI system captured with **owner** and **purpose**?
2. Is **risk class** documented with **reasoning**?
3. For high-risk, is **Annex IV** documentation **workable**, not only slides?
4. Are **deployer duties** (logs, incidents) assigned?
5. Are **changes** (model update, data source) **versioned**?

Common mistakes:

- **"We only call an API"** - ignoring deployer duties and documentation.
- **"Excel is enough"** - no durable history.
- **"Vendor handles everything"** - no proof that **your** role and **your** data flows are covered.

Appendix A: Simplified role matrix

Topic	Provider-typical	Deployer-typical
Intended purpose	In documentation	Match to internal policy
Data	Training/test documentation	Purpose limitation, DPAs
Risk	Risk management system	Operational controls
Logging	Specification	Operations, retention
Incidents	Fix pathways	Escalation, reporting
Changes	Change log / reassessment	Production approvals

Appendix B: Annex III deep-dive (practical)

Use a **two-step test**:

1. Does a use case **literally** match (e.g., recruitment, creditworthiness, critical infrastructure)?
2. Are **exceptions** or overlaps with other regimes relevant?

Document assumptions explicitly - audits move faster when uncertainty is visible.

Keywords: Annex III high-risk AI, recruitment AI, biometric categorization.

Appendix C: FAQ

Q: Is a vendor DPA enough for the AI Act?
A: Contracts help, but they do not replace **technical documentation** and your **risk assessment** of your usage.

Q: Must we inventory every chat tool?
A: For governance, yes; for legal obligations, it depends on risk and role - but without inventory you cannot decide.

Q: What is the difference between "AI software" and an "AI Act Compliance Platform"?
A: Software can be a feature; a **platform** connects **process, data, evidence, and exports** into a repeatable compliance path.
