SimpleAct UG (haftungsbeschränkt)
Tannenstraße 2a · 45661 Recklinghausen
simpleact.de

EU AI Act Compliance Guide

Publisher: SimpleAct · https://simpleact.de
Version: 1.2
Contact: info@simpleact.de · support@simpleact.de
As of: November 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.*

Core problem and the SimpleAct framework

Core problem

Organizations often face the EU AI Act without a continuous chain from transparency to evidence:

- Obligations are known, 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 (document management, 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	Traceable change history (audit log); 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 (often called the EU AI Act) sets binding requirements for AI systems in the Union. Its aims include a high level of protection of health, safety, and fundamental rights, and a functioning internal market for AI.

Key building blocks in everyday organizational work:

Term	Short meaning
AI system	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments (Art. 3(1) AI Act).
Provider	Develops an AI system or has it developed and places it on the market or puts it into service under its own name or trademark.
Deployer	Uses an AI system under its authority (except non-professional or private use).
Importer / distributor	Supply-chain roles with specific duties depending on context.
High-risk AI	Systems covering use cases listed in Annex III that meet the relevant criteria (and do not fall under exceptions), or systems that are a product or a safety component of a product covered by Annex I and subject to third-party conformity assessment (Art. 6 AI Act).
Conformity assessment	Process demonstrating compliance with applicable obligations (varies by risk class and product type).
Technical documentation	Evidence package, especially for high-risk AI (including the Annex IV structure).
Post-market monitoring	Ongoing monitoring after placing on the market or putting into service.
GPAI	General-purpose AI models with a dedicated chapter and transparency and systemic-risk rules.

2. Risk ladder and obligation logic

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

Unacceptable risk

Certain practices are prohibited (for example, depending on design: certain social scoring constructs, real-time remote biometric identification in publicly accessible spaces for law enforcement under Art. 5(1)(h), alongside e.g. points (g) and (e), each with the exceptions set out in the legal text). This is not a matter of fine-tuning, but of not using the prohibited form.

High-risk AI

High-risk applies where Annex III use cases are relevant (for example critical infrastructure, education, employment, essential private and public services, law enforcement, justice, democratic processes, each within the limits set by the legal text) and the high-risk criteria are met. A second path runs through Art. 6(1) and Annex I, where a third-party conformity assessment is required (from 2 August 2028). 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

Limited risk

Primarily transparency obligations (for example, informing users, labeling AI-generated content), subject to legal interpretation. Practical examples: chatbots and AI-generated content (Art. 50 AI Act).

Emotion recognition does not generally belong in this tier. In the workplace and in education institutions, using AI systems to infer emotions is prohibited, except for medical or safety reasons (Art. 5(1)(f) AI Act). Otherwise, emotion recognition systems, in so far as their use is permitted under Union or national law, are high-risk AI systems (Annex III, point 1(c) AI Act). In addition, deployers inform the persons exposed of the operation of the system (Art. 50(3) AI Act).

Minimal risk

No specific obligations under the AI Act; AI literacy under Art. 4 applies to all AI systems. Voluntary transparency and internal governance still help.

3. Roles: provider, deployer, supply chain

Provider

Typical duties include technical documentation, conformity processes, CE marking (where product law applies), quality management, and incident reporting, depending on product and risk class.

Deployer

Deployers must, among other things, ensure appropriate human oversight, control inputs and use according to purpose, keep logs (where required), report serious incidents without undue delay first to

the provider, then to the importer or distributor and the competent market surveillance authority (Art. 26(5); the reporting obligation under Art. 73 falls on the provider; for personal data, Art. 33 GDPR in addition). A deployer that makes a substantial modification to a high-risk AI system may itself become a provider (Art. 25(1) AI Act). Purchased AI still matters: you may be a deployer even if you do not train models.

Importers and distributors

Verify conformity, labeling, documentation, and handoff to downstream actors, and align closely with procurement and the legal team.

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 and testing, where relevant)
- Risk management and post-market processes
- Cybersecurity and lifecycle management

Annex IV provides a structuring framework for the content of the technical documentation. The binding framework is the text of the AI Act. Harmonised standards are voluntary; applying them gives a presumption of conformity (Art. 40(1)) once their references are published in the Official Journal.

Conformity assessment: for Annex III points 2–8 internal control only (Annex VI). For point 1 (biometrics), the choice between Annex VI and VII is open only where harmonised standards or common specifications have been applied in full; otherwise a notified body is mandatory. For Annex I it follows the relevant product law.

5. GPAI and transparency

GPAI models may trigger transparency and documentation duties and rules for models with systemic risk, depending on whether you are an upstream model provider, a system provider, or a downstream actor. For SaaS and software vendors, the chain from base model to product features to tenant configuration determines responsibility splits.

6. Timelines and transition

The regulation introduces staggered applicability (prohibitions, GPAI rules, high-risk obligations, product-related links). Run internal roadmaps and keep a central register of AI systems so deadlines and evidence are managed together, not just once.

Legal position (Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744, Art. 113 and Art. 111; as of November 24, 2026):

- The prohibition of certain practices (Art. 5) and the AI literacy obligation (Art. 4) have applied since February 2, 2025. Art. 4 was replaced by Regulation (EU) 2026/1744; the amended text,

under which providers and deployers take measures to support the development of AI literacy, has applied since that regulation entered into force on July 27, 2026. The prohibitions inserted by Regulation (EU) 2026/1744 under Art. 5(1)(ba) and (bb) (AI systems that, without express consent, generate or manipulate realistic intimate or sexual depictions of identifiable persons, or child sexual abuse material) apply from December 2, 2026.

- The rules for general-purpose AI models (Chapter V) have applied since August 2, 2025. Models placed on the market before that date have until August 2, 2027.
- The general date of application was August 2, 2026; the transparency obligations under Art. 50 have also applied since that day. For generative AI systems placed on the market before then, Art. 50(2) applies only from December 2, 2026.
- The obligations for high-risk AI systems under Annex III apply from December 2, 2027, and under Annex I from August 2, 2028. The prohibitions under Art. 5 apply regardless of these deadlines, with the dates stated above.

7. How SimpleAct helps: the AI Act compliance platform

SimpleAct is not just a single-purpose app. It is a platform for AI Act compliance: a continuous workflow from AI inventory and risk classification through structured documentation and traceable evidence with a change history (audit log) to exportable audit reports.

Why a platform rather than a single 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 and accountability: Ownership and approvals align with governance expectations.

Contrast with generic software

- Ticketing tools track tickets, not risk class or Annex IV documentation.
- Document management systems store files, not structured AI system metadata with compliance versioning.
- ML platforms focus on training and deployment, not regulatory evidence chains.

Coverage map

Area	Value
AI inventory	Full capture, including the risk of unapproved AI use (shadow AI).
Risk classification	Guided mapping to EU categories with Annex III awareness.
Documentation	Structure for technical documentation and operational evidence.

Exports and reports	Evidence packs for audit, management, and external reviewers.
Traceability	Changes are traceable, not “the PDF from last week.”

Pricing: from €159/month billed annually (€199/month billed monthly), excl. VAT. 7-day free trial, no credit card (see simpleact.de/pricing).

8. Glossary (selection)

Term	Explanation
Fundamental rights impact assessment (Art. 27 AI Act)	Obligation of certain deployers of Annex III high-risk AI systems before deploying them: bodies governed by public law, private entities providing public services, and deployers of systems under Annex III, points 5(b) and (c) (creditworthiness, life and health insurance); Annex III, point 2 is excluded. Applies together with the Annex III high-risk obligations from December 2, 2027 (Art. 113(3)(c) AI Act).
Notified body	Conformity assessment by a notified body (Art. 3(22); Annex III point 1 biometrics where standards or common specifications are not applied in full; under product law for Annex I).
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 an owner and purpose?
2. Is the risk class documented with reasoning?
3. For high-risk systems, is the 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.
- “The vendor handles everything”: no proof that your role and your data flows are covered.

Appendix A: Simplified role matrix

The following table helps clarify in workshops who must deliver which artifacts. It does not replace legal review of individual cases.

Topic	Provider-typical	Deployer-typical
Intended purpose	In documentation	Match to internal policy
Data	Training and test documentation	Purpose limitation, data processing agreements
Risk	Risk management system	Operational controls
Logging	Specification	Operations, retention
Incidents	Fix pathways	Escalation; for serious incidents inform the provider, importer or distributor and the market surveillance authority (Art. 26(5))
Changes	Change log, reassessment	Production approvals

Appendix B: Annex III deep-dive (practical)

Annex III lists areas of application in which AI systems may be classified as high-risk, provided the conditions set out there are met. In practice, a two-step test is useful:

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

Document assumptions explicitly. Audits move faster when uncertainty is visible.

Appendix C: FAQ

Q: Is a vendor data processing agreement 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. Without an inventory, however, you cannot decide.

Q: What is the difference between AI software and an AI Act compliance platform?

A: Software can be a single feature; a platform connects process, data, evidence, and exports into a repeatable compliance path.
