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

EU AI Act for SaaS and Software Vendors

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 typical questions for SaaS and software vendors under the EU AI Act. For contracts, products, and roles, involve your legal and compliance team.*

Core problem and the SimpleAct framework

Core problem

SaaS and software vendors face speed-to-market and regulatory pressure at once:

- Provider and deployer roles and multi-tenancy are hard to keep aligned in documentation and contracts.
- Release cycles and model updates break static documentation folders.
- Customer context (industry, proximity to high-risk) must be traceable per tenant.
- Supply chains (general-purpose AI models, subprocessors) rarely form a continuous evidence trail.

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. SaaS context

AI-enabled SaaS products combine:

- A central platform and multi-tenancy
- Fast releases and feature flags
- Customer industries with different risk profiles (e.g., HR vs. support chatbot)

The EU AI Act requires clarity: which component is high-risk, who documents, and how updates remain traceable.

Legal position: The obligations for high-risk AI systems under Annex III apply from December 2, 2027, and under Annex I from August 2, 2028 (Art. 113(3)(c) of the AI Act as amended by Regulation (EU) 2026/1744). August 2, 2026 (Annex III) and August 2, 2027 (Annex I) had previously been scheduled. The prohibitions in Art. 5 have applied since February 2, 2025; the prohibitions added by Regulation (EU) 2026/1744 in Art. 5(1), first subparagraph, points (ba) and (bb) (and paragraphs 1a/1b) apply from December 2, 2026 (Art. 113(3)(a)).

2. Roles in B2B

Role	Typical question
Provider (you)	Do you place the AI system on the market or put it into service?
Deployer (customer)	Does the customer use it under its own authority?
Importer	If relevant in the supply chain

3. Product architecture and risk

- Separate the base model, the product layer, and the customer configuration.
- Document limitations per industry use case (e.g., no automatic final decision without a human, depending on the product).
- Explicitly review Annex III scenarios when customers enable vertical modules.

4. Contracts: DPA, subprocessors

- Subprocessor list and AI-specific schedules
- Purpose limitation
- Audit and inspection rights

- Incident notification and SLAs

5. Releases and substantial modifications

For model updates or new AI features:

1. Trigger the change process
2. Reassess risk
3. Update documentation and customer-facing release notes
4. For high-risk systems: in case of a substantial modification, carry out a new conformity assessment (Art. 43(4); internal control for Annex III points 2–8). Changes to a system that continues to learn, pre-determined by the provider, are not a substantial modification.

6. Multi-tenant isolation

- Technical and organizational tenant isolation
- Logging per tenant
- Feature flags per customer

7. General-purpose AI models

The duties for GPAI models (Arts. 53, 55) fall on the model provider; Chapter V has applied since 2 August 2025, for legacy models until 2 August 2027. If you only integrate such a model, documentation chains and your own role matter most. Confirm with your legal team.

8. Transparency obligations under Art. 50

Since August 2, 2026, the transparency obligations under Art. 50 AI Act have applied, regardless of the risk class. Two of them matter most for SaaS providers:

- **Chatbots and AI assistants (Art. 50(1)):** As the provider, you design the system so that people are informed that they are interacting with an AI, unless this is obvious to a reasonably well-informed, observant person.
- **Synthetic content (Art. 50(2)):** Audio, image, video and text content generated or manipulated by AI must be marked in a machine-readable format and be detectable as artificially generated or manipulated. For systems placed on the market before August 2, 2026, this obligation applies only from December 2, 2026 under the transitional rule of Regulation (EU) 2026/1744.

As deployers, your customers have obligations of their own (Art. 50(3) and (4), such as disclosing deepfakes). Provide them with notice texts and documentation for this.

9. Common SaaS mistakes

- "The customer is always the deployer" is often too simplistic.

- No version history for AI components
- Marketing promises more than the documentation supports.

10. Product checklist

- Inventory of all AI modules
- Risk per module and per vertical template
- Documentation pack for high-risk scenarios
- Incident process with customer communication
- Training for customers on deployer duties

11. Glossary

Term	Meaning
Tenant	Customer partition in multi-tenant SaaS
Feature flag	Toggles features per customer

12. Deep dive: customer success and compliance

- Onboarding checklist (data classes, use cases)
- Regular checks of documented against actual usage
- Quarterly reviews with compliance metrics

13. How SimpleAct helps

SimpleAct is an AI Act compliance platform for inventory, risk, documentation, and exportable evidence, scalable across releases and tenants.

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

Appendix A: Contract clauses (align with legal)

- Service description for the AI feature vs. the base product
- Liability caps and SLA for model availability
- Regulator notification roles for serious incidents

Appendix B: SaaS release checklist

- Customer-facing changelog

- Risk reassessment
- Documentation updated
- Security review for API changes

Appendix C: Industry examples (key terms)

Industry	Annex III proximity	Note
HR / recruiting	Annex III point 4(a)/(b); exception Art. 6(3), never with profiling	human oversight
Finance / credit	creditworthiness of natural persons (point 5(b)), life and health insurance of natural persons (point 5(c))	additional financial regulation
Support chatbot	Art. 50(1)	transparency

Appendix D: FAQ

Q: Must customers draw up technical documentation? A: As a rule, no. That is a provider obligation (Art. 11, Annex IV AI Act). Deployers have their own duties under Art. 26 AI Act: use in line with the instructions for use, monitoring, reporting risks and serious incidents, keeping logs under their control for at least six months and, as employers, informing workers' representatives and affected workers before workplace use. Customers take on provider obligations only if they become providers themselves, for example through a substantial modification (Art. 25(1) AI Act).

Appendix E: Integration patterns and traceability

Pattern	Typical risks	Documentation focus
REST API (sync)	Latency, timeouts	Request/response schema, error codes
Batch / ETL	Data quality, drift	Schedules, sampling, monitoring
Streaming	Real-time hallucinations	Rate limits, human escalation
Embedded SDK	Customer version split	Minimum version, deprecation policy

Practice: Each integration style needs a dedicated section in the technical documentation (interfaces, limits, test evidence).

Appendix F: Short glossary

Term	Meaning in SaaS context
Deployer	Usually the customer; for high-risk AI, own duties under Art. 26, not Art. 11
Provider	You as the product vendor

Substantial modification	May trigger a new conformity path
FRIA (fundamental rights impact assessment)	Fundamental rights; often linked with the DPIA