EU AI Act for SaaS and Software Vendors

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

Keywords: EU AI Act SaaS, B2B software AI, provider deployer, multi-tenant, DPA subprocessor, GPAI

Core problem and the SimpleAct framework

Core problem

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

- **Deployer vs. provider** and **multi-tenancy** are hard to keep aligned in **docs** and **contracts**.
- **Release cycles** and **model updates** break **static** documentation folders.
- **Customer context** (industry, high-risk proximity) must be traceable **per tenant**.
- **Supply chains** (GPAI, **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	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. 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 bot)

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

---

2. Roles in B2B

Role	Typical question
Provider (you)	Do you place/provide the AI system?
Deployer (customer)	Does the customer use it under its authority?
Importer	If relevant in the supply chain

Terms: downstream customization, customer fine-tuning, API-only usage.

---

3. Product architecture and risk

- Separate **base model**, **product layer**, and **customer configuration**
- Document **limitations** per industry use case
- Explicitly review **Annex III** scenarios when customers enable vertical modules

---

4. Contracts: DPA, subprocessors

- Subprocessor list and AI-specific schedules
- **Purpose limitation**

- Audit/inspection rights
- Incident notification and SLAs

Keywords: Art. 28 GDPR processor agreement, TOMs, international transfers.

---

5. Releases and substantial modifications

For model updates or new AI features:

1. Trigger **change**
2. Reassess **risk**
3. Update **documentation** and customer-facing **release notes**
4. Re-check **conformity** pathway

---

6. Multi-tenant isolation

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

---

7. GPAI models

If you integrate **GPAI**: transparency duties, documentation chains, and possibly systemic-risk topics depending on role - confirm with legal.

---

8. Common SaaS mistakes

- "Customer is always deployer" - often **too simplistic**
- No **version history** for AI components
- **Marketing** promises exceed **documentation** depth

---

9. Product checklist

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

---

10. Glossary

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

---

11. Deep dive: customer success + compliance

- Onboarding checklist (data classes, use cases)
- Health checks for documented vs. actual usage
- Quarterly reviews with compliance metrics

---

12. SEO keyword clusters

EU AI Act software vendor, AI Act B2B SaaS, high-risk AI SaaS, Annex III recruitment, AI vendor documentation.

---

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 €199/month.

Appendix A: Contract anchors (align with legal)

- **Service description** for AI feature vs. 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 (keywords)

Industry	Annex III proximity	Note
HR / recruiting	often high	human oversight
Finance / credit	often high	additional financial regulation
Support bot	often limited	transparency

Appendix D: FAQ

Q: When must customers document themselves?
A: When they are **deployers** and bring **their own** data/configurations.

Appendix E: Extended keywords

B2B AI compliance platform, SaaS AI Act documentation, multi-tenant AI logging, EU AI Act customer obligations, vendor AI risk.

Appendix F: 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 deserves a **dedicated section** in technical documentation (interfaces, limits, test evidence).

Appendix G: Short glossary

Term	Meaning in SaaS context
Deployer	Often the customer for on-prem-style configuration
Provider	You as the product vendor
Substantial modification	May trigger a new conformity path

FRIA	Fundamental rights; often linked with DPIA
