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

Template: AI System Inventory (AI Register)

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 template does not replace legal review. It helps you capture and classify AI systems. Binding classification is made case by case with legal and compliance.*

Core problem and the SimpleAct framework

Core problem

Without a reliable inventory there is no basis for risk classification and evidence:

- Shadow AI and supplier APIs stay partly invisible.
- Excel and ad hoc lists are neither traceable with a change history nor audit-ready.
- The mapping from system to risk class is often missing.
- There is no single reliable source for owners, versions, and data flows.

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. Purpose

An AI inventory is the foundation for risk classification, prioritization, and evidence for internal and external reviews.

Legal position: The AI Act does not require a general internal register of all AI systems in use. An inventory is a practical means of meeting related duties, for example clarifying roles and risk classes (Art. 3, 5, 6, 50) or measures for AI literacy (Art. 4, no documentation duty). Source: Regulation (EU) 2024/1689.

2. Master data (required fields)

Field	Description
System ID	Unique ID within the organization
Name	Product or model name
Vendor	Supplier
Version	Software or model version
Owner	Business owner
Department	Using organizational unit
Purpose	Business use case
Data types	Personal data? Sensitive?
Interfaces	API, SaaS, on-premises

3. Risk and EU AI Act

Field	Notes
EU risk class	prohibited (Art. 5) / high-risk (Art. 6, Annex I/III) / transparency obligation (Art. 50) / no specific obligations (Art. 4 applies to all); GPAI separate (Ch. V)
Rationale	Short and auditable
Annex III	Does a listed use case apply?
General-purpose AI model link	Base model or fine-tuned?

4. Technology and operations

Field	Description
Hosting region	EU / non-EU
Model type	LLM, vision, tabular, ...
Training	In-house / vendor / API-only
Monitoring	Drift, quality
Backup / availability	if relevant

5. Compliance and contracts

- Data processing agreement (DPA) in place?
- Subprocessors known?
- Retention periods defined?
- Access restrictions (RBAC) enforced?

6. Shadow AI and detection

Shadow AI: tools without IT approval. Mitigations: allowlists, network monitoring, training, a reporting channel.

7. Review cadence

Frequency	Action
Quarterly	Sample the inventory
On release	Register new systems
On incident	Update the record

8. Example row (anonymized)

System ID	Name	Vendor	Purpose	Risk
AI-014	HR assist	Vendor X	Pre-screening of applications	High (Annex III)

9. Checklist

- [ ] All known AI systems captured
- [ ] Owner assigned
- [ ] Risk rationale documented

- [ ] Contracts linked
- [ ] Next review date set

10. Glossary

Term	Meaning
Asset register	Catalog of digital assets
Data lineage	Traceability of data flows

11. Deep dive: data flow

1. Source → raw data
2. Processing → features / prompts
3. Model → output
4. Use → decision / UI
5. Storage → logs, retention

12. How SimpleAct helps

SimpleAct provides a structured inventory with risk classes and exports as part of an AI Act compliance platform.

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: Extended optional fields

Field	Why
Business criticality	Prioritization under constraints
Personal data exposure	Privacy focus
Model provider region	Third country: adequacy decision Art. 45 (e.g. EU-US DPF) / SCC Art. 46 + TIA
Cost center	Internal chargeback

Appendix B: Sample matrix "department × risk"

Department	Systems count	High-risk (estimate)
HR		
Sales		

Engineering		

Appendix C: FAQ

Q: How often to refresh? A: Quarterly and on every new tool onboarding.

Q: What about "shadow GPT"? A: Treat it as an incident, register it, and tighten the policy.

Appendix D: Data quality rules

- Avoid duplicate records for the same API instance under different names
- Normalize vendor strings (e.g., "OpenAI" vs. "api.openai.com")
- Link to CMDB or ITSM IDs

Appendix E: Access, permissions, and logging

Aspect	Inventory field / note
Authentication	SSO, API keys, service accounts: who may call the model?
Authorization	Role model (RBAC/ABAC), least privilege
Logs	Retention, tamper resistance, access limited to authorized roles
Key rotation	Cadence and owners

Without a clear access chain, evidence for monitorability and incident response is often missing. Capture these points for every production AI system.
