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

Template: Technical Documentation (EU AI Act · Annex IV)

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 structure 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.*

Core problem and the SimpleAct framework

Core problem

Technical documentation under the EU AI Act stays abstract without a shared skeleton:

- Annex IV and Art. 11 are hard to fill without a unified outline.
- Teams duplicate sections each version without clear versioning and change logic.
- Gaps across engineering, legal, and operations stay open.
- Export-ready packages for reviewers are slow to assemble manually.

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

This template helps structure technical documentation content. 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. Fill in fields only when they apply to your system.

Legal position: The technical documentation under Art. 11 and Annex IV of the AI Act is an obligation of providers of high-risk AI systems. It must be drawn up before the system is placed on the market or put into service and kept up to date. Deployers are not subject to it, unless they become providers themselves under Art. 25. The obligation applies from December 2, 2027 (Annex III) or from August 2, 2028 (Annex I). Small and medium-sized enterprises, including start-ups, and small mid-cap enterprises may provide the information in simplified form using a form, once the Commission has published it. Some fields in this template, such as intended users or a change history of the documentation, are practical additions and are not in the wording of Annex IV. Source: Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744, Art. 11(1), Art. 16, Annex IV.

2. System identity

Field	Content / example
Name / version	
Manufacturer / provider	
Deployer (if different)	
Intended purpose	
Deployment scope (regions, environments)	
Interfaces (API, UI, batch)	

3. Annex IV structure (fields)

3.1 General description

- Short description

- Intended purpose and intended users
- Limitations and known failure modes
- Interactions with other systems

3.2 Development and design

- Methods (e.g., supervised learning, RAG, rules)
- Architecture reference
- Configuration summary

3.3 Data for training, validation, testing

- Data provenance
- Preprocessing
- Bias mitigation (where relevant)
- Data quality controls

3.4 Performance and testing

- Metrics (domain-appropriate)
- Test datasets and edge cases
- Known weaknesses

3.5 Cybersecurity

- Threat model (short)
- Access control, encryption
- Logging approach

3.6 Lifecycle

- Versioning
- Update process
- Post-market monitoring

3.7 Further Annex IV items

- Human oversight measures and technical monitoring (point 3)
- Risk management system (point 5)
- Standards applied (point 7)
- EU declaration of conformity (point 8)

4. Deployer-specific add-ons

If you are a deployer, document operational context, logging, internal controls, and incident escalation. This is a practical recommendation, not a requirement of Annex IV.

5. Pre-submission checklist

- Purpose and limits are explicit
- Risk class referenced
- Data sources traceable
- Tests and metrics described
- Security addressed
- Change history maintained

6. Common gaps

- Marketing text instead of technical depth
- No test strategy
- Vendor PDFs not contextualized for your deployment

7. Glossary

Term	Short
Annex IV	Content structure of the technical documentation
Validation	Model and system validation
Human oversight	Human control of the system

8. Deep dive: data categories

Category	Questions
Training data	Provenance, rights, quality
Operational data	Personal data, purpose limitation
Test data	Representativeness, leakage avoidance

9. Deep dive: risk and errors

- False positives and negatives per use case
- Drift and monitoring
- Fallbacks and human escalation

10. How SimpleAct helps

SimpleAct is an AI Act compliance platform that guides you through structured templates and risk prompts and exports the results, instead of loose files per version.

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: Boilerplate snippets (edit for your system)

Purpose (example): "The system assists [role] in [task] by processing [inputs] and producing [outputs]. It is not intended for [unsupported use]."

Limitations (example): "Known limits include [language], [domain], [data volume]. Users must apply [human review] for [decision]."

Appendix B: Legal/compliance review prompts

1. Is the purpose consistent with marketing and contracts?
2. Are the personal data flows described correctly?
3. Is the risk class aligned with the Annex III review?
4. Are subprocessors and third-country transfers covered?

Appendix C: Metrics table template

Metric	Target	Method	Last run
Precision		Hold-out	
Recall			
Latency p95		Load test	

Appendix D: Cybersecurity deep dive

- Short STRIDE-style threat sketch

- Least privilege for API keys
- No secrets in repositories
- Incident response playbooks with AI-specific escalation
