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

Checklist: AI Governance in Your Organisation

Publisher: SimpleAct · https://simpleact.de
Version: 2.1
Contact: info@simpleact.de · support@simpleact.de
As of: November 2026 · Not legal advice

> ***Legal notice:*** *This checklist gives a structured overview. It does not replace a legal assessment of your specific case. The deadlines reflect the situation as of November 2026, including the changes made by the Digital Omnibus (Regulation (EU) 2026/1744). Check the current legal situation before making decisions.*

What you need organisationally to steer AI systems safely and to prove compliance with the AI Act

How to use this checklist

The checklist walks you through AI governance in ten steps: from an overview of the systems you use to the evidence you need for audits. Each step has items to tick off. At the end of each section you see the provision it refers to.

Ideally, go through it together with IT, data protection, the business units and one accountable person from management. A first pass takes about two hours.

Deadlines at a glance

Since / from	What applies	Who is affected
2 Feb 2025	Prohibited AI practices (Art. 5), e.g. social scoring, emotion recognition in the workplace	all providers and deployers
2 Feb 2025	AI literacy (Art. 4): take measures so that staff use AI competently. Since 27 July 2026 (Digital Omnibus) an obligation to promote, without a fixed level per person	every organisation that uses AI
2 Aug 2025	Obligations for providers of general-purpose AI models (Art. 53 et seq.)	model providers, e.g. of large language models
2 Aug 2026	Transparency obligations (Art. 50): AI must identify itself as AI, AI-generated content must be marked	providers and deployers of chatbots, voice assistants, generative AI

2 Dec 2026	End of the transition period for machine-readable marking in systems already in use (Art. 50(2))	providers of generative AI systems placed on the market before 2 Aug 2026
2 Dec 2026	New prohibitions added by the Digital Omnibus (Art. 5(1)(ba) and (bb) and Art. 5(1a) and (1b))	all providers and deployers
2 Dec 2027	Obligations for high-risk AI under Annex III, e.g. recruitment, creditworthiness, critical infrastructure, access to essential services	providers and deployers of these systems

High-risk AI as a safety component of products (Annex I) has its own, later deadline: the obligations apply from 2 August 2028. Fines (Art. 99): up to €35 million or 7% of worldwide annual turnover for prohibited practices; up to €15 million or 3% for breaches of certain other obligations (para. 4); up to €7.5 million or 1% for incorrect or incomplete information to authorities. For SMEs and start-ups the lower amount applies in each case (para. 6). The AI Act itself provides no separate fine bracket for Art. 4 (Art. 99(4)). Since the Digital Omnibus, however, Member States can penalise any infringement (Art. 99(1) as amended); in Germany Art. 4 is currently not subject to fines (§ 15 KI-MIG).

1 · Overview: which AI do we use?

No overview, no control. The first step is a register of all AI systems, including the small tools business units introduced on their own.

- [ ] All AI systems are recorded in one central register, including AI features in existing software (e.g. office suite, CRM, ERP)

Proven approach: ask the business units briefly and cross-check with IT data (licences, SaaS access)

- [ ] For each system, purpose, provider, version and data used are described
- [ ] Each system has a responsible person (system owner)
- [ ] It is clear whether personal data is processed, and the link to the record of processing activities under Art. 30 GDPR is made
- [ ] There is a rule for reporting new AI tools before they are used
- [ ] Unapproved use ("shadow AI") is detected and addressed, not just prohibited

> Basis for all further obligations of the AI Act; Art. 30 GDPR

2 · Classification: what risk does each system carry?

- [ ] Each system has been checked for prohibited practices (Art. 5)
- [ ] Each system is classified: high-risk, transparency obligation, minimal risk

Classification depends on the purpose, not the product: a language model can be harmless in customer service and high-risk in candidate selection

- [ ] For high-risk systems, the Annex III area is named, or it is justified why an exception under Art. 6(3) applies
- [ ] For chatbots, voice assistants and generative AI it is clear which paragraphs of Art. 50 apply
- [ ] The classification is documented with reasons and date and is reviewed whenever something changes

Art. 5, Art. 6, Art. 50, Annex III

3 · Role: provider or deployer?

This determines which obligations you carry yourself.

Role	When	Core obligations
Provider	You develop an AI system or have it developed and place it on the market or put it into service under your own name or trademark, including for your own use	For high-risk: risk management, technical documentation, conformity assessment, registration. For Art. 50: build marking into the product
Deployer	You use another provider's AI system under your own responsibility	Use as intended, human oversight, keep logs, inform affected persons, fundamental rights impact assessment where required (Art. 26, 27)

- [ ] The role is defined and justified for every system
- [ ] It has been checked whether your own modifications, your own name or a changed purpose make you a provider instead of a deployer (Art. 25)
- [ ] For purchased systems, the provider's documents are available (instructions for use, declaration of conformity for high-risk)

Art. 3(3) and (4), Art. 16, Art. 25, Art. 26

4 · Accountability: who decides what?

Task	Carries out	Decides	Is consulted
Maintain the AI register	System owners	Head of IT	Data protection
Classify risk	System owners	Compliance / AI officer	Legal, data protection
Approval before use	Business unit	Management or committee	IT security, legal
Report and handle incidents	Operations / IT	Compliance	Legal, authority if needed
Training	HR	Management	Business units

Example distribution. Adapt the roles to your organisation. What matters is that each task has exactly one person who makes the final decision.

- [ ] There is a named person or function for AI governance (e.g. AI officer)
- [ ] Accountability at management level is clear
- [ ] With several sites or companies, it is clear what is decided centrally and what locally

5 · Rules: AI policy and training

- [ ] There is an AI policy: permitted tools, prohibited uses, handling of confidential and personal data
- [ ] All staff who use AI know the policy
- [ ] There are measures for AI literacy (Art. 4), matched to role and risk: basics for everyone, more depth for system owners and oversight
- [ ] Training is documented (who, when, what content)

> Art. 4

6 · Suppliers and models

- [ ] For each AI provider it is recorded which data goes to them and where it is processed
- [ ] Where personal data flows, a data processing agreement is in place (Art. 28 GDPR); for transfers to third countries the legal basis (adequacy decision, standard contractual clauses)
- [ ] For large language models it is known which model is used and which documents the model provider makes available
- [ ] The contract states whether inputs may be used for training

> Art. 25, Art. 53; Art. 28 and 44 et seq. GDPR

7 · Approval and changes

1. **Report:** a new AI system or AI feature is reported
2. **Review:** classification, role, data protection, IT security
3. **Approval:** before production use; for high-risk we recommend a second person (four-eyes principle)
4. **Re-review:** regularly (recommended: at least once a year) and on every substantial modification

- [ ] The approval process is defined and followed
- [ ] It is defined which changes trigger a new review (new model, new purpose, new data source), and the review checks whether a "substantial modification" exists (Art. 3(23))
- [ ] Approvals are documented with date and person

8 · Transparency under Art. 50 (already applies)

- [ ] Chatbots and voice assistants make clear at the start that they are AI (para. 1)
- [ ] AI-generated text, images, audio and video are marked in a machine-readable way where you are the provider (para. 2). For existing systems by 2 December 2026 at the latest
- [ ] Deepfakes and AI-generated text on matters of public interest are disclosed as AI-generated (para. 4)

Exception for text: no disclosure needed if a human has reviewed it and holds editorial responsibility

- [ ] Where emotion recognition or biometric categorisation is used, the persons concerned are informed (para. 3)

> Art. 50

9 · Incidents and monitoring

- [ ] It is defined how errors, complaints and incidents involving AI are reported
- [ ] For high-risk systems, the reporting route for serious incidents to the authority is clear (Art. 73)

Applies in practice only with the high-risk deadlines from 2027; prepare now

- [ ] Where personal data is affected, the data breach process applies (notification where feasible within 72 hours, Art. 33 GDPR)
- [ ] AI systems are monitored in operation: quality, error rate, unusual results

10 · Evidence: what an audit wants to see

- [ ] Register of all AI systems with classification, role and owners
- [ ] Reasons for the classifications, with date
- [ ] AI policy and training records
- [ ] Approvals and change history
- [ ] For high-risk: technical documentation, risk management, declaration of conformity, registration, fundamental rights impact assessment where required
- [ ] All documents are versioned and can be exported quickly on request, not as loose files in folders

Quick check for management

Five questions every management team should be able to answer:

1. How many AI systems do we use, and which of them are high-risk or fall under Art. 50?
2. Who is responsible for AI governance, and who approves new systems?
3. Are our chatbots and AI content marked, and what still has to happen by 2 December 2026?
4. How do we promote our staff's AI literacy, and can we prove it?
5. Could we hand all evidence to an authority or a customer within one week?

Terms

Term	Meaning
AI system	A machine-based system that infers from its input how to generate outputs such as predictions, content, recommendations or decisions (Art. 3(1))
Provider	Whoever develops an AI system or has it developed and places it on the market or puts it into service under their own name or trademark (Art. 3(3))

Deployer	Whoever uses an AI system under their own responsibility (Art. 3(4))
High-risk AI	AI in sensitive areas under Annex III or as a safety component under Annex I
Shadow AI	AI tools used without the organisation's knowledge or approval
Four-eyes principle	An approval needs a second person who did not submit it

Questions or comments on this checklist?

We keep developing it and welcome feedback: info@simpleact.de. If you would rather not keep these items in spreadsheets: SimpleAct lets you manage register, classification, approvals and evidence in one place, simpleact.de.

Sources: Regulation (EU) 2024/1689 (AI Act); Digital Omnibus on AI, Regulation (EU) 2026/1744; Regulation (EU) 2016/679 (GDPR); KI-MIG (Federal Law Gazette 2026 I no. 223). As of November 2026. Not legal advice.
