AI Act: what do you owe for each AI system, and by when?

This quarter, list every AI system you use, build or sell with your role and its risk class, and check that none is banned and that chatbots and AI content are disclosed as required since 2 August 2026. Then prepare the duties for any Annex III use, such as hiring or credit scoring, before they apply on 2 December 2027.

Reviewed	Next review	Version
4 Nov 2026	**4 Dec 2026**	**1.1**

Written for
Compliance, legal, security and IT leads in EU organizations that use or build AI, including providers of AI systems and models

Latest version
sheets.einblick.dev/ai-act/

If you only do five things

1. **List every AI system and your role in it.**
   Record owner, vendor, purpose, data and who it affects, and whether you are provider, deployer, importer or distributor[1]. Running a chatbot you built under your name makes you its provider[3].
2. **Rule out the banned practices.**
   Eight have applied since February 2025, including emotion recognition at work: tracking call center staff's emotions is banned, tracking customers' is high-risk[1,5]. AI that makes intimate deepfakes without consent is banned from 2 December 2026[2].
3. **Disclose AI where the law requires it.**
   Since 2 August 2026, deployers must disclose deepfakes, and AI text published on public-interest matters that no one edited under editorial responsibility[1]. Customer chatbots must say they are AI; internal assistants for trained staff needn't[3].
4. **Train staff by role and keep a record.**
   Since July 2026 you must support AI literacy, not guarantee a level[2]. Give everyone the basics and people who configure or oversee AI more, and keep attendance lists.
5. **Find your Annex III uses now.**
   Hiring, staff management, credit scoring, life and health insurance pricing, education and remote biometric identification are high-risk uses[1]. Their duties start on 2 December 2027[2].

Classify one AI system

1. **Is it an AI system at all?**
   Software that only runs rules people defined, plain spreadsheets and forecasts that just use averages are not[6]. Mark them out of scope.
2. **Which role do you hold?**
   Provider if you develop it, or have it developed, and supply or run it under your name; deployer if you use it[1]. Rebranding or substantially modifying a high-risk system, or turning a general-purpose one to a high-risk use, makes you its provider[1].
3. **Is the use banned or high-risk?**
   Check Article 5 and Annex III. An Annex III system isn't high-risk if it only does a narrow procedural or preparatory task, improves finished human work or flags deviations for human review, unless it profiles people; the provider documents this and registers the system[1].
4. **Does a disclosure duty apply?**
   Chatbots, generated content, deepfakes and emotion recognition each carry one[1]. Record the result, the reasoning and a review date in the inventory.

What each role owes

Deployer dates are also on the agentic AI sheet.

Deployers (most organizations)

- **High-risk, from 2 December 2027.** Follow the instructions for use, assign trained oversight staff with authority, keep logs at least 6 months, report serious incidents to the provider and the authority, and inform workers and the people affected[1].
- **Impact assessment.** Public bodies, providers of public services and users of credit scoring or life and health insurance pricing assess fundamental rights impacts before first use and notify the authority[1].

Providers of AI systems

- **Chatbots and generative AI.** Say it is AI unless that is obvious. Mark generated content machine-readably; systems on the market before 2 August 2026 have until 2 December 2026[1,2].
- **High-risk, from 2 December 2027.** Risk management, data governance, documentation, logging, human oversight, accuracy and cybersecurity, a quality management system, conformity assessment, CE marking and registration[1]; from 2 August 2028 in products under EU safety law[2].
- **Systems already on the market.** Covered only after a significant design change, or by 2 August 2030 if public authorities use them[2].
- **Incidents.** Report serious ones within 15 days, 10 days after a death and 2 days for a widespread infringement or critical infrastructure disruption[1].

Providers of general-purpose AI models

- **Who.** Indicatively, providers of models trained with over 10^{23} FLOP that generate language, images or video, and anyone fine-tuning one with over a third of its original training compute[7].
- **Duties since 2 August 2025.** Documentation, information for downstream providers, a copyright policy and a public training-content summary; open-source models skip the first two unless systemic. Models placed earlier comply by 2 August 2027[1]. The Commission deems the Code of Practice an adequate voluntary way to show compliance[8].
- **Systemic risk.** Presumed above 10^{25} FLOP: evaluations with adversarial testing, risk mitigation, incident reporting and cybersecurity[1].

What changed in 2026

- **The Digital Omnibus on AI took effect on 27 July 2026.** It moved Annex III high-risk duties from 2 August 2026 to 2 December 2027, softened AI literacy, added the intimate-deepfake ban and extended SME relief to small mid-caps[2,1].
- **Transparency guidance arrived.** A code of practice of 10 June covers marking and labeling[4]; draft guidelines approved on 20 July give examples[3].
- **The first harmonized standard was published.** Since October 2026, EN 18286 gives high-risk providers a presumption of conformity for quality management[9].

Who enforces it, and in Germany

- **Fines scale with the duty.** Up to €35 million or 7% of worldwide turnover for banned practices, €15 million or 3% for most other duties and €7.5 million or 1% for misleading authorities[1].
- **The AI Office handles general-purpose AI.** It can fine model providers up to 3% or €15 million since 2 August 2026, and supervises most systems built on their own models[1,2]. National authorities do the rest[1].
- **Germany: the Bundesnetzagentur.** Since 29 July 2026 it is the default market surveillance authority, contact point and complaints office; BaFin covers AI tied to regulated financial activities[10].
- **Germany: the works council.** Inform it in time about planned AI use; it co-determines tools able to monitor behavior or performance[11,12].

Where the AI Act meets the GDPR and the CRA

- **Build on the DPIA.** High-risk deployers use provider information for their DPIA[1], and the fundamental rights impact assessment may cross-reference it[2].
- **Ask where the model came from.** Models trained on personal data aren't always anonymous. Check that a model wasn't developed unlawfully, starting with its data sources and any regulator findings[13].
- **Bias testing has a legal basis.** Special categories of personal data may be processed where strictly necessary to find and correct bias, under safeguards such as pseudonymization[2].
- **CRA compliance can cover AI cybersecurity.** A high-risk system whose CRA declaration of conformity shows it meets the CRA's essential requirements is deemed to meet the AI Act's cybersecurity requirement[2].

What you can skip

- **ISO/IEC 42001 certification as AI Act proof.** Only EN 18286, which can be layered on ISO/IEC 42001, gives a presumption of conformity for a quality management system[9]. Deployers need neither.
- **Inventorying macros and fixed-rule workflows.** They aren't AI systems[6].
- **AI literacy exams and certificates.** The law asks for measures, not a guaranteed level[2].
- **Labeling internal drafts.** Posts on internal networks and professional correspondence aren't published[3].

Mistakes that cost the most

- **Building CV screening on a general assistant.** It can make you the provider of a high-risk system, with every provider duty[1].
- **Emotion analytics on staff.** Inferring employees' or candidates' emotions from calls or meeting video is banned, even during probation[5].
- **Relying on the vendor's compliance.** Oversight, logs and worker information are deployer duties[1]. Put instructions for use, log access and incident notice in the contract.

What this looks like at your size

Small team, no security staff

- Keep the inventory in a spreadsheet: tool, owner, purpose, data, role and risk class.
- Publish a one-page AI policy (see the AI inputs sheet) and run a short AI basics session each year.
- In Germany, use the guidance the Bundesnetzagentur provides for SMEs and start-ups[10].

Growing, with IT or security staff

- Name one owner for AI governance and send new AI uses through a short intake form.
- Run the AI Act check, the DPIA and the vendor review as one workflow.
- Map Annex III uses and plan oversight training before December 2027.

Enterprise or regulated

- Run AI governance in an existing management system such as ISO/IEC 42001, and add EN 18286 for high-risk systems you provide[9].
- Prepare fundamental rights impact assessments for credit scoring, insurance pricing and public services[1].
- Track fine-tuning compute against the one-third threshold for general-purpose models[7].

Version history

4 Nov 2026, version 1.1	Marked the Commission's Article 50 transparency guidelines as a draft: their content is approved, but they aren't formally adopted yet.

Sources

1. Regulation (EU) 2024/1689 (AI Act), as amended, Articles 3, 5, 6, 25 to 27, 50 to 55, 73, 74, 88, 99, 101, 111, 113, Annex III. EUR-Lex, 27 Jul 2026. eur-lex.europa.eu
2. Regulation (EU) 2026/1744 (Digital Omnibus on AI), Articles 1 and 4. EUR-Lex, 24 Jul 2026. eur-lex.europa.eu
3. Draft guidelines on Article 50 transparency obligations, C(2026) 5054. European Commission, 20 Jul 2026. digital-strategy.ec.europa.eu
4. Code of Practice on Transparency of AI-generated Content. European Commission, updated 19 Oct 2026. digital-strategy.ec.europa.eu
5. Guidelines on prohibited AI practices, C(2025) 5052. European Commission, 29 Jul 2025. digital-strategy.ec.europa.eu
6. Guidelines on the definition of an AI system, C(2025) 5053. European Commission, 29 Jul 2025. digital-strategy.ec.europa.eu
7. Guidelines on obligations for general-purpose AI model providers, C(2025) 7719. European Commission, 19 Nov 2025. digital-strategy.ec.europa.eu
8. The General-Purpose AI Code of Practice. European Commission, updated 7 Oct 2026. digital-strategy.ec.europa.eu
9. First harmonised standard supporting the AI Act published in the Official Journal. European Commission, 19 Oct 2026. digital-strategy.ec.europa.eu
10. KI-MIG, Sections 2, 6, 8 and 12. Federal Ministry of Justice and Consumer Protection (Germany), 22 Jul 2026. gesetze-im-internet.de
11. BetrVG, Sections 87 and 90. Federal Ministry of Justice and Consumer Protection (Germany), as amended 19 Jul 2024. gesetze-im-internet.de
12. Decision 1 ABR 7/15 (co-determination over monitoring devices). Federal Labour Court (Germany), 13 Dec 2016. bundesarbeitsgericht.de
13. Opinion 28/2024 on certain data protection aspects of AI models. European Data Protection Board, 17 Dec 2024. edpb.europa.eu