CLAIRSMITH

AI Act checklist for small businesses

For a business that uses AI (deployer), not one that develops or sells it.

ALREADY APPLIES

- [ ] **Train the people who use AI**
  Take measures to support the AI literacy of your team and of the people using AI on your behalf (guidance, training), in line with their knowledge, experience and the intended use. No specific level is required of any individual.
  Art. 4(1) (as worded by Regulation (EU) 2026/1744) · obligation since 2 February 2025

- [ ] **Check that no use is prohibited**
  Subliminal or deceptive manipulation, exploiting vulnerabilities, social scoring, predicting offences by profiling, facial recognition databases built by scraping, emotion recognition at work or school, sensitive biometric categorisation, real-time remote biometric identification for law enforcement.
  Art. 5(1)(a) to (h) · since 2 February 2025

TRANSPARENCY

- [ ] **Disclose deepfakes**
  If you publish AI-generated or manipulated images, audio or video that are deepfakes, say so. For clearly artistic, satirical or fictional work, a disclosure that does not get in the way of the work is enough.
  Art. 50(4) · since 2 August 2026

- [ ] **Disclose text published to inform the public**
  AI-generated or manipulated text published to inform the public on matters of public interest must say so, unless a human reviewed it and someone holds editorial responsibility for it.
  Art. 50(4), second subparagraph · since 2 August 2026

- [ ] **Inform the people exposed**
  If you use an emotion recognition or biometric categorisation system, tell the people exposed how it works and comply with the GDPR.
  Art. 50(3) · since 2 August 2026

- [ ] **Check your chatbot**
  An assistant that talks to your customers must tell them they are dealing with AI, unless it is obvious. The duty is on the tool's provider: check that the one you use does it.
  Art. 50(1) · since 2 August 2026

COMING NEXT

- [ ] **Do not generate non-consensual sexual content**
  Prohibited from 2 December 2026: using AI for the purpose of generating or manipulating realistic sexual images, video or audio of an identifiable person without their freely given, informed and explicit consent, or child sexual abuse material (Directive 2011/93/EU).
  Art. 5(1)(ba) and (bb), and Art. 5(1a) · from 2 December 2026

- [ ] **Spot high-risk uses**
  Biometrics, critical infrastructure, education and training, employment and staff management (CV sorting), access to essential services (credit), law enforcement, migration, justice and democratic processes. If you have one: use it as its instructions say and give its oversight to a competent, trained person with the authority to act.
  Annex III and Art. 26(1) and (2) · from 2 December 2027 (postponed)

- [ ] **High-risk use (Annex III)**
  Further obligations apply (Art. 26(3) to (12)). Get expert support before you deploy.
  Art. 26(3) to (12) · from 2 December 2027 (postponed)

Checked on EUR-Lex on 16 October 2026: Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744. Not legal advice. Clairsmith · clairsmith.app