AI compliance checklist

Self-assessment checklist: is your business ready for the AI Act, the DSA and the GDPR?

> One page to know where you stand. Tick each box honestly. If you have more than 3 unticked, it is time to act. General information, not individual legal advice. Edition: June 2026.

Step 1. Which regulations apply to you? (1-minute triage)

- ☐ **I use AI in my activity** (chatbot, text/image generation, tools that make decisions or assign scores) - the **AI Act** applies.
- ☐ **That AI touches personal data** (clients, employees, leads) - the **GDPR** also applies.
- ☐ **I have a website/app where third parties publish content** (comments, reviews, marketplace, forum) - the **DSA** also applies.
- ☐ **My website contains only my own content**, with no third-party content - the **DSA does not apply to me**.

Step 2. Risk level of your AI (AI Act)

- ☐ I have verified that **none** of my tools does something **prohibited** (social scoring, emotion recognition in the workplace, sensitive biometric categorisation, mass facial scraping).
- ☐ I know whether I use **high-risk AI** (HR/CV screening, credit scoring, biometrics). If so, I have an assessment, documentation and human oversight in place.
- ☐ My **chatbots and AI-generated content** disclose that they are AI (transparency, art. 50).

Step 3. Data and contracts (GDPR)

- ☐ I have a clear **legal basis** for each processing activity involving AI (art. 6 GDPR).
- ☐ I have signed a **data processing agreement (DPA)** with each AI provider (OpenAI, Anthropic, Google, etc.) **before** feeding it personal data.
- ☐ I have verified the **international transfer mechanism** if the provider is based outside the EU.

- [ ] I have carried out a **DPIA** where there is profiling, sensitive data, or significant automated decisions.
- [ ] Where there are **automated decisions**, a person can understand and override them (art. 22 GDPR).

Step 4. People (employees and affected individuals)

- [ ] I have provided **documented training** on AI to the staff who use it (art. 4 AI Act, already in force).
- [ ] I have **informed the workforce** (or their representatives) about the AI uses that affect them.
- [ ] There is a **visible channel** through which an affected individual can raise a complaint or challenge a decision.

Step 5. Governance and records (accountability)

- [ ] I have an **inventory** of my AI tools (provider, purpose, data, legal basis, DPA).
- [ ] I have my **own internal AI use policy** (not copied from another company).
- [ ] I keep **logs** of relevant decisions.
- [ ] I have an **incident protocol** (including notification to the AEPD within 72 hours in the event of a breach).
- [ ] I review this inventory **at least once a year**.

Step 6. If I have a website/app with third-party content (DSA)

- [ ] I have a **point of contact** and clear terms of use.
- [ ] I have a mechanism for **notifying and removing unlawful content** (notice and action).
- [ ] When I remove content, I **explain the reason** to the user.
- [ ] I do not use **dark patterns** or unidentified advertising.

The 5 pitfalls that attract the most sanctions

1. AI in HR without a risk assessment or legal basis.
2. Automated decisions without genuine human intervention.
3. Chatbots or deepfakes that do not disclose they are AI.
4. Using third-party AI without a signed DPA.
5. “AI-washing”: claiming AI capabilities the system does not have.

Are there unticked boxes? Those are your to-do list. Start with the inventory (Step 5): without knowing what AI you use, you cannot comply with the rest.

Full dossier, sources and detail by regulation: (link to article). General information, not individual legal advice.