AI compliance guide 2026

AI Compliance Guide for Businesses and Individuals (2026): AI Act, DSA and GDPR

> **What this is.** A practical, verified dossier on what European and Spanish authorities will require of anyone who uses artificial intelligence, runs a website, or processes personal data. It is written so that a business owner, self-employed professional, or private individual can understand what applies to them, what regulators will scrutinise closely, where the pitfalls lie, and how to prepare without overspending or underestimating the risk.
>
> **Disclaimer.** This is rigorous information, not individual legal advice. The regulatory framework for 2026 is still evolving (we flag this where relevant). Edition closed: June 2026.

---

1. TL;DR: does this affect me?

Short answer: **almost certainly yes, but probably less than you fear and in a different way than you expect.**

- **Do you use AI in your business** (a chatbot, a tool that drafts text, scores CVs, or generates images)? The **EU AI Regulation (AI Act)** applies to you, almost always in its lighter form, and the **GDPR** applies if that AI touches personal data.
- **Do you have a website or app where others publish content** (comments, reviews, a marketplace, a forum)? The **Digital Services Act (DSA)** applies to you, normally only its basic obligations.
- **Are you self-employed or a professional who creates content with AI** (videos, voices, images)? The **transparency obligations** apply (you must disclose that the content is synthetic). In **purely personal, non-professional use**, the AI Act does not impose those “deployer” obligations on you, but the prohibitions and other rules remain in force (copyright, personal honour, data protection).

The three regulations coexist and complement each other. You do not choose one: the applicable ones apply simultaneously. The rest of this dossier is the map for understanding which ones and what to do.

---

2. The framework in one page

Regulation	What it governs	Who it primarily targets
AI Act (Regulation EU 2024/1689)	The **use and commercialisation of AI systems**, by risk level	Those who develop AI (providers) and those who use it professionally (deployers)
DSA (Regulation EU 2022/2065)	**Intermediary digital services** and the moderation of third-party content	Hosting services, marketplaces, platforms, search engines
GDPR (Regulation EU 2016/679)	The **processing of personal data** (including when done by AI)	Anyone who processes data about individuals

Key idea: the **AI Act** looks at *what the AI system does*; the **GDPR** looks at *what personal data it touches*; the **DSA** looks at *what happens with content that third parties upload to your service*. A single project can trigger all three.

---

3. The timeline (and the deadline that shifted)

The AI Act applies in a **phased** manner (article 113). What is already mandatory and enforceable:

Date	What comes into force	Status
1 Aug 2024	Entry into force	No obligations yet
2 Feb 2025	**Prohibited practices (art. 5)** + **AI literacy (art. 4)**	✅ In force and enforceable
2 Aug 2025	Obligations for **general-purpose AI models (GPAI)**, governance and **sanctions regime (arts. 99-100)**	✅ In force
2 Aug 2026	**High risk under Annex III** + **transparency (art. 50)** + impact assessments + sandboxes	Default date
2 Aug 2027	High risk embedded in **regulated products (Annex I)**	Default date

🔴 Box: the deadline that shifted

Here is the nuance that almost nobody explains properly. In November 2025, the European Commission proposed the **"Digital Omnibus"** (COM(2025)836), a package that **proposes delaying the entry into force of the high-risk regime**:

- **Annex III** (biometrics, employment, education, essential services, etc.): from 2 Aug 2026 to **late 2027** (sources point to 2 Dec 2027).
- **Annex I** (AI embedded in regulated products): from 2 Aug 2027 to **2028** (around 2 Aug 2028).

But note: as of June 2026, this is a **proposal under legislative procedure** (procedure 2025/0359(COD)), **not applicable law**: the text has not yet been definitively adopted or published in the Official Journal of the EU, and the exact dates may change during negotiations. The Omnibus "moves the clock, not the architecture": it does not change the substance of the obligations, only when they begin.

What to do with this: plan conservatively towards August 2026, because the delay is not yet certain, but factor in that you will probably have more time than the default calendar suggests. Verify the final dates before making major decisions. Source: Digital Omnibus, European Commission.

What really matters today: **the prohibitions and the training obligation have been in force since February 2025.** They are not future requirements.

---

4. The AI Act by risk level

The AI Act classifies AI systems into four levels. Your first task is to know which level each tool you use falls into.

🚫 Unacceptable risk (prohibited), art. 5

Eight practices prohibited since February 2025, with no possible mitigation. Those most likely to affect businesses:

- Subliminal manipulation or exploitation of vulnerabilities to alter behaviour in a harmful way.
- **Social scoring** of individuals.
- **Emotion recognition in the workplace and in educational institutions** (except for medical or safety reasons).
- **Biometric categorisation** based on sensitive characteristics (race, religion, sexual orientation, etc.).
- Creating facial recognition databases through **mass scraping** of the internet or cameras.

If any tool in your business does any of the above, the answer is not to “mitigate” it: the tool must be withdrawn.

⚠️ High risk (Annex III + Annex I)

Systems in eight sensitive areas: biometrics, critical infrastructure, **education**, **employment and HR** (CV screening, promotion decisions), essential services (including **credit scoring**), law enforcement, migration and justice. If you develop one of these, the obligations are extensive: risk management, data governance, technical documentation, log-keeping, human oversight, robustness, conformity assessment, **CE marking** and registration in an EU database.

If you only use one (you are a “deployer”), your obligations are more limited but real: use it according to the instructions, designated **human oversight**, keep **logs (minimum 6 months)**, **inform workers’ representatives**, and, in certain cases, carry out a **Fundamental Rights Impact Assessment (FRIA, art. 27)**.

💬 Limited risk (transparency), art. 50

The level where most SMEs will fall. Main obligation: **notify**.

- A **chatbot** must identify itself as AI (“you are speaking with an automated assistant”).
- Whoever **develops** a system that generates synthetic content must label it in a machine-readable format (art. 50.2). Whoever **publishes a deepfake** must **disclose that it has been generated or manipulated using AI** (art. 50.4), with specific carve-outs for creative, satirical or artistic works.

These transparency obligations apply from **August 2026**. Note: the Digital Omnibus delay affects the **high-risk regime** (Chapter III), not these obligations under art. 50 (except for a specific transition for generative systems already on the market). Implementing them early is good practice and is often already required by consumer protection rules.

✅ Minimal risk

Spam filters, video games, trivial recommendation engines. No specific AI Act obligations.

> **General-purpose AI models (GPAI):** if you use ChatGPT, Claude, Gemini or similar, *you* are not their provider, so the GPAI obligations (technical documentation, training data summary, copyright policy; and for the most powerful models, red-teaming and incident reporting) fall on the company that develops them, not on you. They affect you as a *deployer* at whichever risk level corresponds to your use.

---

5. DSA: do I have a “platform”? (and why you probably do not)

The DSA worries SMEs more than it should. What really matters:

- **Corporate website with no third-party content:** the DSA **does not apply to you**, because you are not an “intermediary service” (the DSA only regulates those who host or transmit third-party content). Your obligations come from the GDPR and consumer protection rules, not the DSA.
- **Website with comments or reviews:** you become a “hosting service”. Basic obligations: **a mechanism for notifying and removing unlawful content** (notice and action, art. 16) and **providing reasons** when you remove something (art. 17).
- **Marketplace or forum:** you are an “online platform”, but here is the relief: **article 19 exempts micro and small enterprises** (fewer than 50 employees and less than €10 million in turnover) from the heavier obligations (formal complaints system, out-of-court dispute resolution, transparency reports). It does **not exempt** you from notice and action or from providing reasons for removals.
- **Very large online platform (VLOP):** from 45 million users in the EU. Audits, risk assessment, direct supervision by the Commission. This is not your situation if you are reading this.

Sanctions: up to **6% of global annual turnover** (art. 74). For large platforms (VLOPs) these are imposed by the European Commission; for other intermediary services, national authorities set them (art. 52), also up to that 6%. The DSA has been **fully applicable since 17 February 2024**.

> **A detail almost nobody mentions:** in Spain, the DSA authority is the **CNMC** (Digital Services Coordinator), but the European Commission **brought proceedings against Spain before the Court of Justice of the EU in May 2025** (IP/25/1081) because the CNMC still **does not have full enforcement powers**. The DSA is directly applicable regardless, but the administrative fines regime in Spain is still being put in place. Translation: the obligation exists; the national enforcement stick is still being assembled.

Do not confuse the DSA with the GDPR (data) or the DMA (large platforms and competition): they are different regulations.

---

6. Who is watching and what they will scrutinise

Authorities:

Authority	Scope
AI Office (European Commission)	General-purpose AI models (GPAI); EU coordination
AESIA (Spanish Agency for AI Supervision, A Coruña)	Prohibited practices, general high risk, transparency
AEPD	Personal data, **biometrics**, automated decisions (art. 22 GDPR)
CNMC	DSA and competitive dimension of algorithms

AESIA exists and is operational (established by RD 729/2023), and has already concluded the **first regulatory AI sandbox in the EU**. Its full enforcement powers depend on the future **Spanish Organic Law on the good use and governance of AI**, which as of June 2026 is still **under legislative procedure, not yet in force**.

Enforcement priorities (what they will look at first):

1. **Prohibited** practices (social scoring, biometrics, manipulation). Already sanctionable.
2. **Transparency**: chatbots and deepfakes without disclosure.
3. **High-risk systems without conformity** (HR, scoring) lacking documentation or human oversight.
4. **Intersection with the GDPR**: legal basis, automated decisions, impact assessments.
5. **Complaints from affected individuals**: inspections often start from a complaint.

---

7. Sanctions: how much it hurts

AI Act (art. 99), verified figures:

Conduct	General regime (the higher amount)	SMEs (the lower amount)
Prohibited practices (art. 5)	**€35 million or 7%** of global turnover	the lower of the two
Breaching other obligations	**€15 million or 3%**	the lower of the two
Providing incorrect information to authorities	**€7.5 million or 1%**	the lower of the two

Two important and little-known points: the incorrect information tier is **1%** (not 1.5%, as some sources repeat), and for **SMEs and start-ups the lower of the two amounts applies** (the opposite of the rule for large companies). Detail in article 99.

DSA: up to **6%** of global annual turnover (the European Commission for large platforms; national authorities for other intermediary services).

GDPR: up to **€20 million or 4%**. In Spain, the AEPD resolved hundreds of enforcement proceedings in 2024; AI features among its declared priorities.

---

8. The pitfalls (typical mistakes that attract sanctions)

Listed by regulatory severity:

1. **AI in HR without an assessment.** Screening CVs or deciding on promotions with AI is high risk: it requires a legal basis, an impact assessment and human oversight. Doing it blindly is a triple infringement.
2. **Automated decisions without genuine human intervention** (art. 22 GDPR). The human must be able to understand and override the system, not simply rubber-stamp whatever the machine says.
3. **Biometrics without a reinforced legal basis** (art. 9 GDPR). In the employment context, employee consent in Spain is not considered valid due to the power imbalance.
4. **A chatbot that does not disclose it is AI** (art. 50).
5. **Using a third-party AI without a signed data processing agreement (DPA)** before feeding it personal data. Liability falls on you, not on the provider.
6. **Mass scraping of personal data for AI** without a balancing test. The EDPB Opinion 28/2024 is clear: legitimate interest does not automatically prevail.
7. **Deepfakes and synthetic content without labelling.**
8. **Failing to inform the workforce** of an AI use that affects them (art. 64 of the Spanish Workers' Statute + arts. 13-14 GDPR).
9. **"AI-washing"**: marketing capabilities the system does not have (misleading advertising).
10. **Copying another company's AI policy.** This breaches the accountability principle and aggravates the sanction if there is an inspection.

---

9. Good vs bad practices

Aspect	Bad	Good
AI inventory	Informal, “I already know what I use”	Register with provider, purpose, data and legal basis per tool
Automated decisions	No human review possible	Designated person who can override + visible challenge channel
Chatbot	Presents itself as a person	“I am an AI assistant” from the first message
AI-generated content	No label	Visible label + technical marking in metadata
AI provider	API without a signed DPA	DPA signed before the first call involving personal data
Training	“They already know how to use AI”	Signed record, proportionate to risk, kept up to date
Oversight	“The system is very good”	Person who understands and can override; documented
Incidents	Wait for a customer complaint	Protocol: detect, assess, notify AEPD within 72 hours

The common thread is the **accountability principle**: it is not enough to comply, you must **be able to demonstrate and justify it** to the authority with living documentation.

---

10. How to prepare your business: a phased checklist

Block A. Inventory (do this now). List every AI tool you use: provider, purpose, data it touches, legal basis, and whether a DPA has been signed.

Block B. Legal basis and contracts (before processing data). A GDPR legal basis (art. 6) for each processing activity; a **signed DPA** with each AI provider (OpenAI, Anthropic and Google all offer these); verify the international transfer mechanism (EU-US framework or standard contractual clauses).

Block C. Impact assessments (before deploying). Carry out a **DPIA** if there is profiling, special category data, or significant automated decisions. Add a **FRIA** (art. 27) if you are a **public body**, a **private entity providing public services**, or you use high-risk AI to **assess the creditworthiness or credit scoring** of individuals or for **life and health insurance** (Annex III.5).

Block D. Transparency (before August 2026). “You are speaking with AI” notice on chatbots; label for AI-generated content; mechanism for challenging automated decisions.

Block E. Training (art. 4, already in force). Documented training signed by each employee, proportionate to the risk of their role. No official certification is required, but a record must be kept.

Block F. Oversight and records (ongoing). Decision logs, genuinely documented human oversight, annual inventory review, and an incident protocol (notification to AEPD within 72 hours in the event of a breach).

---

11. For individuals and self-employed professionals

It is not only businesses that are in the crosshairs:

- **Content creators using AI in a professional capacity:** the obligation to **disclose synthetic content** (art. 50) applies when you publish deepfakes, AI-generated voices or images in the context of a professional activity. Purely personal and domestic use falls largely outside the AI Act, though not outside other rules.
- **Deepfakes without consent:** in addition to the transparency requirement, certain uses (sexual, impersonation) are prohibited or specifically regulated by law. The forthcoming Spanish law reinforces this.
- **Copyright:** generating something with AI does not automatically make you the rights holder, and using third-party works to create content may have legal consequences.
- **Self-employed professionals who use AI with client data:** the same GDPR rules and DPA obligations with the provider apply to you as they do to a company.

---

12. Quick glossary

- **Provider:** the entity that develops or markets the AI system.
- **Deployer:** the entity that uses the AI system in its activity. Most businesses.
- **GPAI:** general-purpose AI model (the large generative models).
- **DPIA:** data protection impact assessment (GDPR, art. 35).
- **FRIA:** fundamental rights impact assessment (AI Act, art. 27).
- **DPA:** data processing agreement (GDPR, art. 28).
- **VLOP:** very large online platform (DSA).
- **Accountability:** proactive responsibility; being able to demonstrate compliance.

Sources

> For article numbers and sanctions, the authoritative source is always the **official text in EUR-Lex / Official Journal of the EU**. Analysis pages (such as artificialintelligenceact.eu) are included only for explanatory support, not as a

> normative source.

Primary (AI Act) - Regulation (EU) 2024/1689, consolidated text (including arts. 5, 27, 50, 99 and 113): https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es - Application timeline (AI Act Service Desk, European Commission): https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act - Digital Omnibus, proposal COM(2025)836 (European Commission): https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

Explanatory support (non-official) - AI Act Explorer (article-by-article analysis, arts. 27/50/99): https://artificialintelligenceact.eu/es/

DSA - Regulation (EU) 2022/2065, text: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32022R2065 - DSA policy (European Commission): https://digital-strategy.ec.europa.eu/en/policies/digital-services-act - VLOP/VLOSE list: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops - CNMC, Digital Services Coordinator: https://www.cnmc.es/en/sectores-que-regulamos/servicios-digitales-dsa - Commission proceedings against Spain (IP/25/1081): https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081

Spain / GDPR - AESIA (official website): https://aesia.digital.gob.es/es - RD 729/2023 (AESIA statute): https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18911 - AEPD, guide on adapting AI processing to the GDPR: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf - AEPD, guidance on agentic AI: https://www.aepd.es/guias/orientaciones-ia-agentica.pdf - EDPB, Opinion 28/2024 (AI models and data protection): https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

Cases - Fine by the Italian Garante against OpenAI (€15 million, December 2024). Primary source: statement from the *Garante per la protezione dei dati personali* (https://www.garanteprivacy.it). Press coverage (secondary): https://www.euronews.com/next/2024/12/20/italys-privacy-watchdog-fines-openai-15-million-after-probe-into-chatgpt-data-collection

---

Edition closed in June 2026. The regulatory framework is evolving (in particular, the Digital Omnibus and the Spanish Organic Law on AI). Verify dates and the status of legislative proceedings before making decisions with legal implications. General information, not individual legal advice.