



The 31-step compliance checklist

Every step in the order the Act asks for it, grouped by phase, with the provision behind each one. Printed to be worked through with a pen.

31

steps

7

phases

The shape of the work

31 steps across 7 phases. They are not the same size, and the order is not a preference: each phase establishes something the next one needs.

Steps in each phase

01 Establish what you hold		3
02 Screen against the prohibitions		2
03 Classify each system		5
04 Build the high-risk requirements		8
05 Meet the deployer duties		4
06 Clear the route to market		4
07 Operate, monitor and keep it current		5

Phase 01 has no deadline of its own and blocks every phase after it: nothing can be assessed until the inventory exists.

Establish what you hold, and screen against the prohibitions

01 Establish what you hold

Every obligation in the Regulation depends on facts about a specific system, so nothing can be assessed until the inventory exists. This phase has no deadline of its own and blocks every phase after it.

- ☐ **Build a register of every AI system you develop, buy, embed or reach through an API**
Include the intended purpose, the business process it sits in, whether output reaches people outside the organisation, and the vendor. Features added to tools already in use are the most commonly missed category, because no procurement decision marked their arrival.
[Article 3\(1\)](#) · Whoever owns technology risk, with procurement and engineering

- ☐ **Fix your role for each system: provider, deployer, importer or distributor**
Duties attach to roles, not to company types, and one organisation is routinely several at once. A deployer becomes a provider if it puts its own name on a system, substantially modifies it, or changes its intended purpose, which is the single most common scoping mistake.
[Article 3\(3\)-\(7\)](#) · [Article 25](#) · Legal, on engineering's description of what was changed

- ☐ **Confirm territorial scope for each system**
You are in scope if you place a system on the EU market wherever you are established, or if the output is used in the Union. Being outside the EU is not itself an exclusion. Military, defence, national security and purely personal non-professional use are excluded.
[Article 2](#) · Legal

02 Screen against the prohibitions

Article 5 is absolute: a prohibited practice cannot be made lawful by documentation, consent or safeguards. Screen for it before spending effort anywhere else, because a hit means the system cannot be placed on the market or used at all.

- ☐ **Test every system against all ten Article 5 prohibitions**
Eight have been unlawful since 2 February 2025. Two more, non-consensual intimate imagery and child sexual abuse material, apply from 2 December 2026. Any material listing eight prohibitions describes the superseded text.
[Article 5](#) · [Prohibited practices guide](#) · Legal, with the system owner · due 2 Dec 2026

- ☐ **Where a carve-out is relied on, record which one and why it applies**
Several prohibitions have narrow statutory qualifications: notably real-time remote biometric identification for law enforcement. Relying on a carve-out is a documented legal position, not an assumption.
[Article 5\(2\)-\(7\)](#) · Legal
Applies if you rely on any Article 5 carve-out

Classify each system

Classification decides which regime applies and therefore how much work follows. The two high-risk routes carry different deadlines, so the route matters as much as the conclusion.

☐ Check the Annex I product-safety route

A system is high-risk if it is a safety component of a product covered by the Union harmonisation legislation in Annex I, or is itself such a product, and requires third-party conformity assessment under that legislation.

[Article 6\(1\)](#) · [Annex I](#) · Product compliance · due 2 Aug 2028

☐ Check the Annex III use-case route

Eight areas: biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration and border control, and the administration of justice. This route carries the earlier deadline.

[Article 6\(2\)](#) · [Annex III](#) · Legal, with the business owner · due 2 Dec 2027

☐ If you rely on the Annex III derogation, document and register the assessment

A system in an Annex III area is not high-risk if it does not pose a significant risk of harm, on the grounds listed in Article 6(3). Relying on this requires a documented assessment before placing on the market, and registration in the EU database.

[Article 6\(3\)-\(4\)](#) · [Article 49\(2\)](#) · Provider

Applies if you conclude an Annex III system is not high-risk

☐ Check Article 50 separately, in every tier

Transparency duties attach regardless of risk tier wherever a system interacts with people, generates synthetic audio, image, video or text, produces deep fakes, or infers emotion or biometric categories. A minimal-risk system can still owe them.

[Article 50](#) · [Article 50 guide](#) · Product, with legal · due 2 Aug 2026

☐ If you place a general-purpose AI model on the market, assess systemic risk

General-purpose AI models are regulated in their own right under Chapter V, separately from systems built on them. Assess whether the model meets the systemic-risk threshold, and notify the Commission if it does.

[Article 51](#) · [Article 52](#) · Model provider

Applies if you place a general-purpose AI model on the EU market

Build the high-risk requirements

This is the heavy phase and the reason the deferral to December 2027 is a schedule change rather than a reprieve. Each requirement produces evidence that a conformity assessment will look for.

- ☐ **Establish a documented, continuous risk management system**
 Not a one-off assessment: a process that runs across the lifecycle, identifying and evaluating known and reasonably foreseeable risks, and adopting mitigation measures. It has to be documented and maintained.
[Article 9](#) · Provider · due 2 Dec 2027

- ☐ **Apply data governance to training, validation and testing data**
 Covers design choices, collection and origin, preparation, assumptions, availability and suitability, and examination for bias. Article 10(5) permits processing special categories strictly for bias detection and correction, subject to safeguards, and Article 4a broadened that basis.
[Article 10](#) · [GDPR interplay](#) · Data and ML engineering, with privacy · due 2 Dec 2027

- ☐ **Produce technical documentation to the Annex IV specification**
 It must exist before the system is placed on the market and be kept current. Annex IV sets the minimum contents; this is the document a market surveillance authority asks for first.
[Article 11](#) · [Annex IV](#) · Provider · due 2 Dec 2027

- ☐ **Enable automatic logging over the system's lifetime**
 Logs must allow traceability appropriate to the intended purpose. Retention is at least six months unless other Union or national law requires longer.
[Article 12](#) · Engineering · due 2 Dec 2027

- ☐ **Write instructions for use that let a deployer meet its own duties**
 Including the intended purpose, accuracy and robustness levels, known limitations, foreseeable misuse, the human oversight measures required, and expected lifetime and maintenance.
[Article 13](#) · Provider · due 2 Dec 2027

- ☐ **Design human oversight into the system, not around it**
 The person overseeing must be able to understand capacities and limits, monitor for anomalies, resist automation bias, correctly interpret output, decide not to use it, and intervene or stop. A review step that cannot actually override the system does not satisfy this.
[Article 14](#) · [Human oversight guide](#) · Product and engineering · due 2 Dec 2027

- ☐ **Set and declare accuracy, robustness and cybersecurity levels**
 Declared metrics go in the instructions for use. Robustness covers resilience to errors and inconsistencies; cybersecurity covers attempts to alter use, behaviour or performance, including data poisoning and adversarial examples.
[Article 15](#) · Engineering and security · due 2 Dec 2027

- ☐ **Put a quality management system in place**
 A documented system covering regulatory compliance strategy, design and verification procedures, data management, the risk management system, post-market monitoring, incident reporting and accountability.
[Article 17](#) · Provider · due 2 Dec 2027

Meet the deployer duties, and clear the route to market

05 Meet the deployer duties

Most organisations deploy far more systems than they provide, and deployer duties are frequently missed because the provider's documentation is mistaken for the whole obligation.

- ☐ **Use the system in accordance with its instructions, and assign competent human oversight**
Oversight must be assigned to named people with the competence, training and authority to exercise it, and the authority matters as much as the training.
[Article 26\(1\)-\(2\)](#) · Deployer · due 2 Dec 2027

- ☐ **Monitor operation, keep logs, and report serious incidents**
Suspend use and inform the provider where you have reason to consider that use in accordance with the instructions may present a risk. Keep logs for at least six months.
[Article 26\(5\)-\(6\)](#) · [Article 73](#) · Deployer · due 2 Dec 2027

- ☐ **Inform affected people**
Workers and their representatives must be informed before a high-risk system is put into use in the workplace. People subject to a decision informed by an Annex III system must be told the system was used.
[Article 26\(7\), 26\(11\)](#) · HR and the business owner · due 2 Dec 2027

- ☐ **Complete a fundamental rights impact assessment where required**
Required for deployers that are public bodies, or private entities providing public services, and for certain creditworthiness and life or health insurance pricing uses.
[Article 27](#) · Deployer, with legal · due 2 Dec 2027
Applies if you are a public body, provide public services, or score credit or insurance risk

06 Clear the route to market

The gate between a compliant build and lawful placing on the market. Which route applies depends on the classification route and on whether harmonised standards were applied.

- ☐ **Determine the conformity assessment route**
Annex VI internal control, or Annex VII involving a notified body. For most Annex III systems internal control is available where harmonised standards were applied in full; biometrics is the notable exception.
[Article 43](#) · [Conformity assessment guide](#) · Provider · due 2 Dec 2027

- ☐ **Draw up the EU declaration of conformity and affix CE marking**
The declaration is kept for ten years after placing on the market and made available to authorities on request.
[Article 47](#) · [Article 48](#) · [Annex V](#) · Provider · due 2 Dec 2027

- ☐ **Register in the EU database before placing on the market**
Applies to providers of Annex III high-risk systems, to those relying on the Article 6(3) derogation, and to certain public-authority deployers.
[Article 49](#) · [Article 71](#) · Provider · due 2 Dec 2027

- ☐ **Appoint an authorised representative in the Union**
Required for providers established outside the Union, by written mandate, before placing a high-risk system on the market.
[Article 22](#) · Provider · due 2 Dec 2027
Applies if you are established outside the EU

Operate, monitor and keep it current

Compliance is a standing condition, not a launch milestone. These obligations run for as long as the system is on the market.

☐ **Run post-market monitoring against a documented plan**

Proportionate to the nature and risks of the system: collect, document and analyse performance data across the lifetime, and feed it back into the risk management system.

[Article 72](#) · Provider · due 2 Dec 2027

☐ **Establish a serious incident reporting path that meets the deadlines**

Report to the market surveillance authority of the Member State where the incident occurred. The deadlines are short and vary with the nature of the incident, so the path has to exist before it is needed.

[Article 73](#) · Provider, with incident response · due 2 Dec 2027

☐ **Mark synthetic content in a machine-readable format**

Providers of generative systems must mark output as artificially generated or manipulated. Systems already on the market when the transparency rules began have until 2 December 2026 to comply.

[Article 50\(2\)](#) · Provider · due 2 Dec 2026

Applies if your system generates synthetic audio, image, video or text

☐ **Take measures to support AI literacy, and record what you did**

Applies to every provider and deployer regardless of risk tier, and has since 2 February 2025. The Digital Omnibus softened this from ensuring a level of literacy to taking measures to support it, which changes what you should be recording, not whether you owe it.

[Article 4 · AI Literacy Program](#) · HR and the business owner · due 2 Feb 2025

☐ **Re-check guidance published before 27 July 2026**

Regulation (EU) 2026/1744 changed deadlines, added two prohibitions, softened Article 4 and created new AI Office enforcement powers. Deadlines and prohibition counts in older material are likely to be wrong.

[Digital Omnibus changes](#) · Whoever maintains your compliance documentation

Work it in order, and keep the evidence

HOLISTIC AI

The enterprise AI governance platform

Holistic AI governs AI across the lifecycle: an inventory of every system, the classification behind each one, the evidence a supervisory authority will ask for, and continuous monitoring once it is live.

[EU AI Act readiness assessment →](https://holisticai.com/eu-ai-act-readiness)

holisticai.com/eu-ai-act-readiness

[Get a demo →](https://holisticai.com/demo)

holisticai.com/demo

Classify one system

The risk calculator walks the same sequence the Act does and names the provision behind each answer.

euaiact.com/eu-ai-act-risk-calculator

Check your exposure

The readiness check scores the whole estate against the obligations that already bind and the ones that are coming.

euaiact.com/eu-ai-act-readiness



Holistic AI

The EU AI Act, as a working tool

euaiact.com is maintained by Holistic AI as an independent, source-verified reference: the complete legal text with the Omnibus amendments marked, a scope finder, a risk classifier, eight sector guides and a 31-step compliance checklist — all free.

YOUR NEXT STEP

Find out where you actually stand

Classify one system in a few minutes, or have Holistic AI assess the whole portfolio and produce the evidence behind it.

[Classify a system →](#)

[Start the assessment →](#)

euaiact.com/eu-ai-act-risk-calculator

holisticai.com/eu-ai-act-readiness

Or book a walkthrough of the platform: holisticai.com/demo