



THORIAN

# EU AI ACT READINESS CHECKLIST

AI-NATIVE COMPLIANCE. HUMAN ACCOUNTABLE.

LAST UPDATED:

2026-05-22

[WWW.THORIAN.IO](http://WWW.THORIAN.IO)

# EXECUTIVE SUMMARY

## WHY THIS CHECKLIST EXISTS

The EU AI Act is already live. Prohibited practices (Article 5) have been enforceable since February 2025.

GPAI obligations (Articles 53–55) since August 2025 – both with Commission-level fines.

General application of most operator and deployer obligations begins August 2026.

High-risk Annex III systems must be fully compliant by August 2027.

The Act reaches any company whose products, customers, employees, or model outputs touch the EU – not just companies based in Europe.

## WHAT IS INSIDE

**Seven sections:** prohibited practices (A), high-risk classification (B), governance foundations (C, Articles 4–15), GPAI provider obligations (D, Annex XI), transparency (E, Article 50), a deadline calendar (F), and a self-scoring rubric (G).

Vendor-specific questions sit at the top of the document.

## HOW TO USE IT

Tick the boxes. The score ranges in Section G tell you where you sit – whether you need an assessment in 90 days or you are positioned for August 2026. Vendor and supply-chain roles score on a separate scale.

## NEXT STEP

If you score below sixteen across Sections A–E, you need a formal readiness assessment. Thorian delivers inventory, classification, gap analysis, policy templates, and a 10-page readiness report in 30 days for \$4,999 – human auditor sign-off, AI-accelerated analysis.

# VENDORS AND SUPPLIERS

**This section applies if you supply AI components, services, customisation, or software to a company subject to the EU AI Act.** It also applies if you embed, fine-tune, or modify an AI system that is ultimately deployed in the EU.

You do not need to be building an AI system of your own to be here. The Act does not draw the line at ownership. It draws the line at [who](#) puts the output to use inside the EU.

## AI ACT CATEGORY: NAMED OR NOT ANSWERABLE

The Act has 8 Annex III categories plus GPAI. Name the one that applies, or you cannot answer their next question

## AI ACT CLASSIFICATION: CONFIRMED BEFORE SIGNING

You are not guessing what bucket your customer falls in. The 14-month clock starts on classification, not on your readiness.

## MAP YOUR ROLE IN THE SUPPLY CHAIN

You may be provider, deployer, importer, distributor, authorised representative, or a combination. Each role carries distinct obligations. Not knowing which one you are is not a defence.

## AI COMPONENT INSIDE ANNEX III HIGH-RISK

Provider documentation obligations apply to your component regardless of where it sits in the stack. Yours is not a peripheral exception.

## FINE-TUNE FOR EU USERS: A SEPARATE DEPLOYMENT

The tuned instance counts as a separate system from the original model. Documentation requirements start the moment that tuned instance is released in the EU.

## COMPLIANCE POSITION: PRODUCE IT ON REQUEST

Your EU customer or their auditor will want to know what your product does, what data it handles, and what user decisions it influences. If you cannot write this down, the deal is at risk.

## CONTRACTS WITH EU COUNTERPARTIES

AI Act compliance clauses are appearing in EU RFPs now. If your agreement does not address what you represent, you are exposed.

## PENALTY EXPOSURE: UP TO €15M OR 3% OF GLOBAL TURNOVER

Importers, distributors, authorised representatives, and deployers face the same Article 99(4) exposure as providers. The Act reaches every party in the commercial chain, not just the company that built the model.

# SECTION A — PROHIBITED AI PRACTICES

ALREADY ACTIVE, ENFORCEABLE SINCE FEBRUARY 2025. FINES UP TO EUR 35M OR 7% OF GLOBAL REVENUE, WHICHEVER IS HIGHER.

☐

**Real-time remote biometric identification in public spaces.** Facial recognition at events, in transit or in retail. Law-enforcement exceptions are narrow and specific; everything else is prohibited.

☐

**Inferring sensitive attributes from biometrics.** Deriving a person's race, political views, health status, sexual orientation or union membership from biometric data.

☐

**Emotion recognition in the workplace or education environment.** Employee state monitoring, student engagement scoring from facial or voice analysis – prohibited in workplaces and educational settings.

☐

**Large-scale social scoring by public authorities.**  
Prohibited.

☐

**AI that manipulates or exploits vulnerabilities.** Targeting children, elderly people, disabled people or anyone under significant economic duress.

☐

**Predictive criminal risk scoring based on statistical profiling.** Scoring re-offending risk without factual grounding. Prohibited.

☐

**Scraping or open-source mining of biometric databases.**  
Prohibited.



## ONE OR MORE BOXES TICKED?

You are operating a prohibited system. Do not wait for a regulator. The fines are already being issued.

# SECTION B — HIGH RISK SYSTEMS

ANNEX III. THE COMPLIANCE DEADLINE IS **AUGUST 2, 2027**. FINES UP TO 7% OF GLOBAL REVENUE.

The EU AI Act lists eight categories of high-risk AI. Match each of your systems to the correct category by the time you are done with this checklist. The compliance clock starts on the deadline, not on when you begin the assessment.

☐

**Biometric identification or categorisation.** Facial recognition for access control or KYC, emotion analysis, voice biometrics, gait analysis, fingerprint-based inference of sensitive attributes.

☐

**Safety component in critical infrastructure.** AI managing electricity grids, water treatment, gas pipelines, road traffic or industrial safety systems.

☐

**Education and vocational training.** AI evaluating admissions decisions, grading at scale, adaptive learning with assessment, automated exam proctoring, student behaviour monitoring.

☐

**Employment and self-employment access.** AI resume screening, video interview analysis, performance ranking, task allocation, productivity monitoring.

☐

**Essential private and public services.** AI credit scoring, insurance underwriting, eligibility scoring for public benefits, emergency call patient triage, health insurance eligibility.

☐

**Law enforcement.** Evidence evaluation, re-offending risk scoring, criminal investigation pattern analysis, polygraph-type tools.

☐

**Migration, asylum and border control.** Asylum case triage, visa eligibility screening, biometric at borders, risk assessment at border crossings.

☐

**Administration of justice and democratic processes.** Legal research and case law prediction AI, election or referendum targeting, voting behaviour optimisation.

## ONE OR MORE BOXES TICKED?

You have roughly 14 months to get the first assessment done and the documentation in place. The schedule does not wait for you to feel ready.

## SECTION B2 — HIGH RISK FOUNDATIONS

IF YOU TICKED ANY OF THE BOXES IN SECTION B, YOU NEED **ALL** OF THE FOLLOWING ITEMS BELOW.

- ☐ **AI system inventory.** You can name every AI system you run or deploy – its purpose, version, owner and data inputs. 83% of enterprises do not have this.
- ☐ **Risk management system.** Documented process for identifying, assessing and mitigating AI-specific risks before the system goes live and on an ongoing basis. (Article 9.)
- ☐ **Data governance.** Your training and operation datasets are checked for relevance, representativeness, quality and bias. You are logging data provenance and applying appropriate protection. (Article 10.)
- ☐ **Technical documentation.** Annex IV-compliant documentation exists for each high-risk system: system description, architecture, training methodology, test results, monitoring plan. (Article 11 and Annex IV.)
- ☐ **Logging and audit trail.** Your AI system produces automatic logs that you can retain and reproduce for regulators. (Article 12.)
- ☐ **Article 13 transparency.** The natural person subject to an AI decision has been told in plain language what the system is doing and why it is making that decision about them. (August 2026 for most systems.)
- ☐ **Human oversight.** Your high-risk AI has a real review and stop mechanism, not a checkbox. (Article 14.)
- ☐ **Accuracy, robustness and cybersecurity.** Documented measures keep the AI accurate, model-poisoning-resilient and operationally stable. (Article 15.)
- ☐ **CE marking and declaration of conformity.** Assessment is complete and the CE mark and declaration of conformity are in place before the system goes to market. (August 2027 unless derogated.)
- ☐ **Registration in the EU AI database.** Your high-risk system is registered in the EU public database before it goes to market. (Article 49, August 2027. GPAI models are already registered.)

### DOES ANY OF THIS FEEL DAUNTING?

We get it. It's a lot of documentation. That's why we're here to help you prepare for your AI system's debut into the EU market.

# SECTION C — GENERAL PURPOSE AI (GPAI) PROVIDERS

ALREADY ACTIVE SINCE AUGUST 2025. COMMISSION-LEVEL FINES APPLY FROM DAY ONE.

Applies if you build, fine-tune, embed proprietary vector models on top of a foundation model, or train your own from scratch.

- ☐ **Technical documentation.** You can produce Annex XI-compliant documentation on request: model card, capabilities and limitations, training methodology, test methods and training data sources. (Article 53(1)(a).)
- ☐ **Copyright policy.** You have put in place a policy to respect EU copyright – including steps to opt out of copyright reservation under the CDSM Directive – and published a summary of training data sources. (Article 53(1)(b).)
- ☐ **Training data summary.** A public URL-level summary of training data sources exists and is current. (Article 53(1)(b).)
- ☐ **Systemic risk threshold assessment.** You have checked whether your model meets the  $10^{25}$  FLOP threshold. If it does, you notified the EU AI Office within six months. (Article 51.)
- ☐ **Adversarial or red-team testing.** If your model carries systemic risk, you have documented the results. (Article 55(b).)
- ☐ **Serious incident reporting process.** You have a documented process that feeds serious incidents to the EU AI Office and national authorities. (Article 55(d).)
- ☐ **Energy consumption disclosure.** If systemic risk applies, you have documented model energy consumption. (Article 55(a).)
- ☐ **EU AI Office notification.** You notified the EU AI Office before placing your model on the market if it meets systemic risk criteria. (Article 51(3).)

## DOES ANY OF THIS FEEL DAUNTING?

We get it. It's a lot of documentation. That's why we're here to help you prepare for your AI system's debut into the EU market.

# SECTION D — TRANSPARENCY OBLIGATIONS

GENERAL APPLICATION FROM AUGUST 2026. LOWER PENALTY TIER – UP TO EUR 15M OR 3% OF TURNOVER.

☐

**AI-generated content is labelled.** Text, image, video and audio output is marked as AI-generated, including watermarking. (Article 50(1).)

☐

**AI identity disclosed to users.** Chatbots, emotion recognition systems and virtual assistants tell users they are AI. (Article 50(2).)

☐

**Emotion recognition consent.** Emotion recognition has not been used without lawful consent, unless a specific narrow exception applies. (Article 3(34) and Article 50.)

☐

**Biometric categorisation in the workplace and education needs a legal basis.** Any system running without one has enforcement exposure from August 2026 onward.

☐

**Deployer transparency notice.** If you deploy an AI system – reseller, integrator or direct operator – you have confirmed your provider gave you the required instructions for use, and you have told downstream affected persons what system is in use.

## DOES ANY OF THIS FEEL DAUNTING?

We get it. It's a lot of documentation. That's why we're here to help you prepare for your AI system's debut into the EU market.

# SECTION E — THE DEADLINE CALENDAR

| DATE                 | WHAT BECOMES ACTIVE OR REQUIRED                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FEBRUARY 2025</b> | Prohibited practices (Article 5) — already active                                                                                                    |
| <b>AUGUST 2025</b>   | GPAI obligations (Articles 53, 55) — already active, Commission fines in force                                                                       |
| <b>AUGUST 2026</b>   | General application: most operator obligations are live. 3 months away now.                                                                          |
| <b>AUGUST 2027</b>   | Annex III high-risk systems must be fully compliant. CE marking, declaration of conformity, EU AI database registration all due. 15 months away now. |
| <b>AUGUST 2028</b>   | High-risk systems under existing EU product safety legislation (Annex I) fully transitioned.                                                         |

## US COMPANY SELLING HIGH-RISK AI TO EU CUSTOMERS?

If you are a US company selling high-risk AI to EU customers, August 2027 is your date. That is not time for a full gap analysis and remediation cycle. Most companies will need 12 to 18 months. Start now.

# WHAT THORIAN DOES WITH THIS

THE CHECKLIST ANSWERS WHERE YOU ARE. THE ASSESSMENT ANSWERS WHAT NEXT.

## The ball is in your court

### For operators and providers

Map your full obligation stack – inventory, classification, gap analysis, report, policy templates, debrief call.

### For vendors and suppliers

Your EU counterparties are already asking. We build the compliance evidence package – system inventory, Annex III classification, supply-chain role mapping – that your customer's audit team is looking for.

## We deliver in 30 days

- AI system inventory – up to 5 systems
- Annex III risk classification with article citations
- Full gap analysis against Articles 4-50 of the AI Act
- 10-page readiness report with evidence index
- Policy templates: AI governance, risk management, data governance
- 1-hour debrief call with our assessor – SANS/GIAC-certified, 12+ years GRC experience

**4.999 EUR – 30 days** – Your deadline hasn't waited this long. Start now – we finish in 30!

### EU BASED, FOR EU COMPANIES

We are an Estonian-registered EU compliance firm. EU entities and EU law firms prefer to work with EU vendors on EU regulation.