ethyx
ethyx.eu

AI Risk Classification Checklist

EU AI Act (Regulation 2024/1689) · Step-by-step decision tree for deployers · EN

Reviewed by a certified Data Protection Officer (CIPP/E) · Provided by ETHYX · Version 1.1 · July 2026 · Not legal advice

HOW TO USE Work through Steps 1–5 in order for each AI system in your inventory. Stop as soon as you reach an outcome – do not continue to the next step. Complete one checklist per AI system. Keep completed checklists in your AI documentation file.

Ref. (from AI System Inventory):		**System being classified:**	
Completed by:		**Date:**	

Tick any box that applies. If any box is ticked → outcome: PROHIBITED – do not deploy.

STEP 1 Is the system PROHIBITED? (Art. 5 EU AI Act)

- ☐ Subliminal, manipulative or deceptive techniques to distort behaviour in a way that causes or is likely to cause harm (Art. 5(1)(a)).
- ☐ Exploiting vulnerabilities of specific groups (age, disability, social/economic situation) to distort behaviour and cause harm (Art. 5(1)(b)).
- ☐ Biometric categorisation of individuals based on sensitive attributes to infer race, political opinions, trade union membership, religious beliefs, sexual orientation (Art. 5(1)(g)). Exceptions for law enforcement apply – specialist legal advice required.
- ☐ Real-time remote biometric identification (e.g. facial recognition) in publicly accessible spaces for law enforcement (Art. 5(1)(h), with narrow exceptions in (h)(i)-(iii)). Narrow exceptions exist for law enforcement – specialist advice required.
- ☐ Social scoring by public authorities: evaluating individuals based on their social behaviour or personal characteristics for detrimental treatment (Art. 5(1)(c)).
- ☐ Individual criminal risk assessment or prediction of recidivism based solely on profiling (Art. 5(1)(d)).
- ☐ Emotion recognition in workplaces or educational institutions – unless for specific medical or safety purposes (Art. 5(1)(f)).
- ☐ Creating or expanding facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage (Art. 5(1)(e)).
- ☐ AI systems that generate or manipulate non-consensual intimate imagery or child sexual abuse material (Art. 5, added by the 2026 Digital Omnibus; compliance required by 2 December 2026).
- ☐ NONE of the above apply → continue to Step 2. ONE OR MORE apply → OUTCOME: PROHIBITED. Do not deploy this system. Seek legal advice.

Tick any box that applies. One tick = HIGH RISK outcome. Both sub-tests count independently.

2A – Safety component of Annex I regulated product (Art. 6(1)):

STEP 2 Is the system HIGH RISK? (Art. 6, Annex I & III)

☐	Machinery, toys, recreational craft, lifts, explosive atmospheres equipment, radio equipment, pressure equipment, medical devices (incl. in vitro diagnostic), civil aviation, rail systems, motor vehicles, agricultural machinery.
☐	2B – Listed in Annex III (Art. 6(2)) – eight high-risk categories:
☐	Biometric identification and categorisation of natural persons. Excl.: verification, accessibility, safety.
☐	Management and operation of critical infrastructure (power, water, gas, transport, digital).
☐	Education and vocational training: AI deciding or influencing access, admission, assessment, or qualification.
☐	Employment, workforce management, and access to self-employment: recruitment, selection, performance evaluation, promotion, termination, allocation of tasks, monitoring. This is the most common trigger for SMEs – e.g. CV screening, attendance monitoring.
☐	Access to and enjoyment of essential private services and public benefits: credit scoring, insurance risk assessment, emergency services dispatch, social benefits.
☐	Law enforcement: individual risk assessments, polygraphs, evaluation of evidence, crime analytics, profiling.
☐	Migration, asylum and border control management.
☐	Administration of justice and democratic processes.
☐	NONE of the above apply → continue to Step 3. ONE OR MORE apply → OUTCOME: HIGH RISK. Deployer obligations under Art. 26 EU AI Act apply. Complete a Deployer Documentation Pack. Fundamental Rights Impact Assessment (Art. 27) may be required. Fine: up to €15 million or 3% of global annual turnover.

General-purpose AI models are trained on large amounts of data and can serve many tasks (e.g. GPT-4, Claude, Gemini, Llama). As a deployer you are not the provider of the GPAI model – your obligations depend on how you use it.

STEP 3 Is this a General-Purpose AI (GPAI) system? (Art. 51)

☐	You are using a GPAI model or a product built on one (e.g. a chatbot powered by an LLM, Copilot, a recommendation engine).
☐	The GPAI model you use has been listed as a 'systemic risk' model by the EU AI Office (typically: >10^25 FLOPs training compute).

If you ticked the first box: classify the use case using Steps 1–2 and 4. A GPAI model used for internal drafting = minimal risk. The same model used for HR screening = likely high risk. If you ticked the second box: additional obligations may apply – consult your provider's documentation.

Tick any box that applies. Ticking one = transparency obligation, not a prohibition or full compliance burden.

STEP 4 Does a LIMITED RISK transparency obligation apply? (Art. 50)

- ☐ AI chatbot or virtual assistant interacting with humans (unless it is obvious the system is AI).
- ☐ AI system generating synthetic audio, images, video, or text that could be mistaken for real (deepfake or synthetic content).
- ☐ Emotion recognition system or biometric categorisation system (not already high-risk in Step 2).
- ☐ AI-generated content: text, images, audio, video produced by AI and presented to others (labelling required).
- ☐ NONE apply → continue to Step 5. → OUTCOME: LIMITED RISK. Implement transparency disclosure and document it. Fine for non-compliance: up to €7.5 million or 1.5% of global annual turnover.

Art. 50 requires you to clearly inform individuals they are interacting with AI or AI-generated content. Implement a disclosure banner, conversation opener, or label. Use the Deployer Documentation Pack Art. 50 template.

If you reached Step 5, the system does not fall into any higher-risk category. There are no mandatory obligations under the EU AI Act – but responsible use practices apply.

STEP 5 MINIMAL RISK (default for all remaining systems)

- ☐ Document the system in your AI System Inventory with risk classification = Minimal risk.
- ☐ Confirm the intended use is consistent with the provider's permitted use policy.
- ☐ Brief staff on the tool's capabilities and limitations (Art. 4 AI literacy).
- ☐ Review classification annually or if the use case changes significantly.
- ☐ → OUTCOME: MINIMAL RISK. Document and proceed. No mandatory EU AI Act obligations beyond good practice.
- ☐ OUTCOME SUMMARY – Record your classification here
- ☐ Classification outcome: ☐ Prohibited ☐ High risk ☐ Limited risk ☐ Minimal risk ☐ Under review
- ☐ Summary of reason:

_____

- ☐ Next actions required:

_____

- ☐ Reviewed and signed off by: _____ (Name) _____ (Date)

No EU AI Act fine tier for minimal-risk systems – but GDPR may still apply if personal data is processed. Check your AI System Inventory for any GDPR obligations (DPA, ROPA entry, etc.).

This checklist is provided for guidance only and does not constitute legal advice. It is based on Regulation (EU) 2024/1689 (EU AI Act) as amended by the 2026 Digital Omnibus (adopted June 2026; under it, obligations for stand-alone Annex III high-risk systems, including Art. 26/27 deployer duties, apply from 2 December 2027, Annex I from 2 August 2028; Art. 4 AI literacy and Art. 50 transparency are unchanged). Reviewed by a certified Data Protection Officer (CIPP/E). Provided by ETHYX – ethyx.eu. GDPR max fine: €20M / 4% turnover. EU AI Act max fine: €35M / 7% turnover. Version 1.1 · July 2026.