AI Risk & Privacy Assessment

A one-sitting worksheet to classify an AI system under the EU AI Act, map its obligations, and record the privacy and oversight controls before you ship it.

FOR	TIME TO COMPLETE	VERSION
TEAMS BUILDING OR DEPLOYING AI IN THE EU	45-60 MINUTES	JULY 2026

How to use this

Work top to bottom. Fill Section 1 first - your risk tier decides how much of the rest applies. Anything you can't answer is itself a finding: note it in the risk register (Section 6) with an owner. Revisit whenever the system's purpose, data, or user population materially changes.

Why now

The EU AI Act is phased. Prohibited-practice and AI-literacy duties applied from **2 Feb 2025**; GPAI model-provider obligations applied from **2 Aug 2025**. Most remaining obligations apply from **2 Aug 2026**, with Article 6(1) product-safety high-risk systems following from **2 Aug 2027** under the original Act. Implementation dates may change through EU simplification packages, so confirm the current timeline before launch.

1 System snapshot

Describe the system once, plainly. If you can't, that's the first thing to fix.

System / feature name

Internal owner (name & role)

What it does, in one sentence a non-engineer understands

Who / what does it affect? (users, decisions, downstream systems)

Model(s) used (own, fine-tuned, or third-party / GPAI API)

Intended purpose and deployment context (internal, customer-facing, regulated product, public service)

2 Risk classification (EU AI Act)

Tick the first row that matches. Your highest applicable tier governs your obligations.

Check	Tier	Trigger - does the system...	If yes
[ ]	Prohibited	use manipulative/subliminal techniques, social scoring, untargeted facial scraping, emotion inference at work/school, or similar banned uses?	Stop. Do not deploy in the EU.
[ ]	High-risk	act as a safety component, or operate in an Annex III area - biometrics, critical infrastructure, education, employment/HR, essential private/public services, credit, law enforcement, migration, justice?	Full high-risk regime (Sections 3-6).
[ ]	Limited / transparency	interact with people (chatbot), or generate or manipulate image, audio, video or text (incl. deepfakes)?	Disclosure & labelling duties (Section 5).
[ ]	Minimal	none of the above (e.g. spam filter, recommender, internal tooling)?	Voluntary good practice; revisit if scope changes.

Classification note

For Annex III use cases, check whether an exemption applies and document the reasoning. If the system profiles people or could significantly affect them, treat the analysis as high-risk until reviewed.

Determined tier & one-line justification

3 Your role & obligations

The same system carries different duties depending on your role. Tick all that apply.

Check	Role	You are...	Key duties to log
[ ]	**Provider**	developing/placing the system on the market under your name	risk mgmt, data governance, tech docs, logging, human oversight, conformity
[ ]	**Deployer**	using a third-party system under your authority	use per instructions, human oversight, input relevance, monitoring
[ ]	**Importer / distributor**	making another provider's AI system available in the EU	provider checks, documentation, instructions, corrective action
[ ]	**Product manufacturer**	embedding AI in a regulated product under your name	sector rules, conformity route, product technical file
[ ]	**GPAI model provider**	providing a general-purpose model, not just using an API	technical docs, copyright policy, training-data summary; extra duties if systemic risk

If using a third-party model/API: provider, model name/version, terms reviewed, restricted uses

4 Training & inference data review

Bad data is where most AI risk actually lives. Complete one row per significant data source.

#	Data source	Contains personal / special-category data?	Lawful basis / provenance	Bias & quality check
1	e.g. user uploads	Y/N - type	consent / contract / licence	representative? gaps?
2				
3				
4				

Privacy overlap

If any source contains personal data, this AI system almost certainly needs a **Data Protection Impact Assessment**. Use the rdelune DPIA template alongside this one and cross-reference the two.

5 Human oversight & transparency controls

For each control, mark status: Yes / Partial / No. Missing items become risks.

Control	Status	Evidence / where implemented
Users are told they are interacting with AI (not a human)	Y / P / N	
AI-generated / manipulated content is labelled (incl. machine-readable marking)	Y / P / N	
A human can review, override, or stop consequential outputs	Y / P / N	
Decisions and inputs are logged for traceability	Y / P / N	
Accuracy, robustness & failure modes are tested and monitored	Y / P / N	
Users have a route to contest or get an explanation of an outcome	Y / P / N	
Staff and operators have AI literacy/training appropriate to their role	Y / P / N	

6 Technical documentation map & risk register

High-risk systems need technical documentation (Annex IV). Map what exists and log the gaps.

Required artefact	Exists?	Where it lives / owner
System description & intended purpose	[ ]	
Data governance & datasets used	[ ]	
Design, architecture & model choices	[ ]	
Testing, metrics & known limitations	[ ]	
Human-oversight & risk-management measures	[ ]	
Post-market monitoring / incident response owner	[ ]	
Fundamental-rights impact assessment needed?	[ ]	deployer / public body / Annex III trigger check

Open risks & actions

#	Risk / gap	Severity	Action & owner	Due
1		H/M/L		
2				
3				

Need a practical compliance review?

This template gets you started. If you'd like an engineer who does compliance to pressure-test your answers - or turn them into working controls, documentation, and audit-ready evidence - book a free 30-minute discovery call.

Book a free discovery call or visit rdelune.dev

This template is provided by rdelune LLC for general informational purposes only and does not constitute legal, regulatory, or professional advice, nor create a consultant-client relationship. Regulatory obligations depend on your specific facts and jurisdiction. Validate your completed document against the applicable law (e.g. the EU GDPR, the ePrivacy Directive, and the EU AI Act) and, where appropriate, with a qualified professional. © 2026 rdelune LLC. You may use and adapt this template freely within your organisation; please retain this attribution.