EU AI Act Obligations Checker

Work out your role, classify each AI feature, and see which obligations apply and from when, with the article for each. Dates reflect the Digital Omnibus on AI.

How to use

- Step 1: your role. Step 2: classify each AI feature. Step 3: read the obligations for your role and class.
- The Act can apply to US companies when an AI system is placed on the EU market or its output is used in the EU.
- This is a plain-language guide, not legal advice. Check the Official Journal text and get legal review for high-risk systems.

Example answers and mappings are templates, not facts about your company. Edit every bracket and validate each statement before sharing it with a customer or auditor.

Step 1: your role

ID	Step / category	Question or obligation	Article	Applies from	What to do
G01	Scope	Do you place AI systems on the EU market, or is your AI's output used in the EU?	Art. 2	-	If yes, continue. If no, the Act likely does not apply, but EU customers may still ask.
G02	Role	Provider: you develop an AI system or model and put it on the market under your name.	Art. 3	-	Most SaaS companies with their own AI features are providers of those features.
G03	Role	Deployer: you use an AI system under your authority in your work.	Art. 3	-	Your customers are often deployers of your AI features.
G04	Role	Importer or distributor: you bring a non-EU provider's system into the EU market.	Art. 3	-	Check the importer and distributor duties if this applies.

Kailash Consult

Step 2: classify each AI feature

ID	Step / category	Question or obligation	Article	Applies from	What to do
G05	Prohibited	Does any feature manipulate, exploit vulnerabilities, do social scoring, untargeted facial scraping, workplace or school emotion recognition, or similar banned uses?	Art. 5	2 Feb 2025	If yes, stop: these practices are banned.
G06	High-risk (Annex III)	Is the feature used in employment, education, credit scoring, insurance pricing, essential services, biometrics, critical infrastructure, law enforcement, migration or justice?	Art. 6, Annex III	2 Dec 2027	If yes, it is likely high-risk unless the Art. 6(3) exception applies; document the assessment.
G07	High-risk (Annex I)	Is the AI a safety component of a product covered by EU product law (for example medical devices, machinery)?	Art. 6(1), Annex I	2 Aug 2028	If yes, high-risk duties apply through that product's conformity route.
G08	Transparency	Does the feature chat with people, generate text, images, audio or video, or create deepfakes?	Art. 50	2 Aug 2026	Transparency duties apply (see Step 3).
G09	General-purpose AI model	Do you train and release a general-purpose AI model yourself?	Art. 53	2 Aug 2025	Model provider duties apply. Using someone else's model through an API does not make you a GPAI provider.
G10	Minimal risk	None of the above.	-	-	No specific duties beyond AI literacy; voluntary codes encouraged.

Step 3: obligations for everyone

ID	Step / category	Question or obligation	Article	Applies from	What to do
G11	All	Support AI literacy among staff who build or use AI.	Art. 4	2 Feb 2025	Training on your AI policy and AI limits; keep records.

Step 3: transparency obligations

ID	Step / category	Question or obligation	Article	Applies from	What to do
G12	Provider	Tell people when they are interacting with an AI system, unless obvious.	Art. 50(1)	2 Aug 2026	Label chat and assistant features in the interface.

Kailash Consult

ID	Step / category	Question or obligation	Article	Applies from	What to do
G13	Provider	Mark AI-generated audio, image, video and text in a machine-readable way.	Art. 50(2)	2 Aug 2026	Watermarking or metadata. Grace period to 2 Dec 2026 for systems already on the market before 2 Aug 2026.
G14	Deployer	Inform people exposed to emotion recognition or biometric categorization.	Art. 50(3)	2 Aug 2026	Notice before use.
G15	Deployer	Disclose deepfakes and AI-generated text published on matters of public interest.	Art. 50(4)	2 Aug 2026	Visible disclosure.

Step 3: high-risk provider obligations

ID	Step / category	Question or obligation	Article	Applies from	What to do
G16	Provider	Risk management system across the life cycle.	Art. 9	2 Dec 2027	ISO 42001 risk and impact assessment helps here.
G17	Provider	Data governance for training, validation and test data.	Art. 10	2 Dec 2027	Data quality, relevance and bias checks.
G18	Provider	Technical documentation.	Art. 11	2 Dec 2027	Annex IV contents.
G19	Provider	Automatic logging of events.	Art. 12	2 Dec 2027	Logs that allow traceability.
G20	Provider	Instructions for use and transparency to deployers.	Art. 13	2 Dec 2027	Capabilities, limits, intended purpose.
G21	Provider	Design for effective human oversight.	Art. 14	2 Dec 2027	Ability to monitor, override and stop.
G22	Provider	Accuracy, robustness and cybersecurity.	Art. 15	2 Dec 2027	Declared accuracy metrics; resilience to attacks.
G23	Provider	Quality management system, conformity assessment, declaration, CE marking and EU database registration.	Art. 17, 43, 47, 48, 49	2 Dec 2027	ISO 42001 can support the quality management system.
G24	Provider	Post-market monitoring and serious incident reporting.	Art. 72, 73	2 Dec 2027	Monitoring plan; incident process.

Kailash Consult

Step 3: high-risk deployer obligations

ID	Step / category	Question or obligation	Article	Applies from	What to do
G25	Deployer	Use per instructions, assign human oversight, monitor, keep logs at least six months, inform affected workers.	Art. 26	2 Dec 2027	Applies to your customers using high-risk systems.
G26	Deployer	Fundamental rights impact assessment for public bodies and certain deployers such as credit scoring and life or health insurance.	Art. 27	2 Dec 2027	Check whether this applies to you or your customers.

Step 3: general-purpose AI model providers

ID	Step / category	Question or obligation	Article	Applies from	What to do
G27	GPAI provider	Technical documentation, information for downstream providers, copyright policy and a public summary of training content.	Art. 53	2 Aug 2025	Models placed on the market before 2 Aug 2025 have until 2 Aug 2027.
G28	GPAI provider	Extra duties for models with systemic risk: evaluation, incident reporting, cybersecurity.	Art. 55	2 Aug 2025	Applies to the largest models only.

Penalties

ID	Step / category	Question or obligation	Article	Applies from	What to do
G29	Fines	Up to EUR 35M or 7% of global turnover for prohibited practices; up to EUR 15M or 3% for most other breaches; up to EUR 7.5M or 1% for misleading information.	Art. 99	2 Aug 2025	Lower caps apply to SMEs.

Free resource from Kailash Consult. Free to use inside your company. Not for resale or redistribution. kailashconsult.com/resources