EU AI Act compliance for European institutions

Evidence, accountability and operational readiness.

Prepared 8 November 2026 · Vasilios Kotitsas · UberConsul, Frankfurt am Main

A practical working guide for EU institutions, bodies, offices and agencies, and European public-mission organisations. Use it to identify obligations, gather evidence and frame a review with your legal, data-protection, procurement and operational teams.

Read this first

This is an independent advisory publication, not an EU publication, certification, conformity assessment or legal opinion. Completing this guide does not establish compliance. Requirements depend on your role, intended purpose, risk classification, sector and applicable law.

Use current law, not a remembered deadline

The AI Act has phased application, amendments and transitional provisions. Check the current EUR-Lex record, consolidated Article 113 and applicable amendment acts before setting deadlines. An adopted amendment and a proposal are not the same thing. Record the exact version and applicability decision in your evidence register.

A five-part working sequence

1. Establish scope and roles.
2. Classify each use case.
3. Identify the evidence and accountable owner.
4. Resolve gaps before the applicable gate.
5. Monitor change and exercise recovery.

Official legal record: EUR-Lex · Regulation (EU) 2024/1689

01 / Scope and risk classification

Inventory systems, not just vendors

For each system record intended purpose, users, affected people, decision context, data categories, provider, hosting, integrations, accountable owner and deployment status. Include embedded AI and staff-accessible tools. Distinguish the underlying general-purpose model from the system that uses it.

Determine the institutional role

Read Articles 2 and 3. An institution can be a deployer, an AI-system provider, or have different roles for different systems. Development under your name, rebranding, changes of intended purpose and substantial modification can alter duties; examine Article 25 where relevant. Buying a model subscription does not alone make you its GPAI provider.

EU institution or national public body?

The Act expressly covers Union institutions acting as AI-system providers or deployers. Article 70 assigns the EDPS the relevant supervision for Union institutions. For their personal-data processing, assess Regulation (EU) 2018/1725; national public bodies normally assess GDPR and national law. Check any exclusions and sector-specific instruments separately.

Classify intended use

Check Article 5 prohibited practices first. Then evaluate Article 6, Annex I and Annex III, including relevant exceptions. Public-sector use, sensitive data or a powerful model alone does not establish high-risk classification. Document facts, legal basis, reasoning, reviewer and reclassification triggers.

Working evidence

System inventory; role map; classification memorandum; current-law reference and applicability dates; named legal and operational reviewers. Do not apply a high-risk checklist to every system without this assessment.

02 / Duties and operational evidence

Literacy and transparency

Review current Article 4 and applicable staff arrangements; retain role-relevant training and competence evidence without treating a certificate as proof of compliance. Evaluate Article 50 notices, disclosures and technical marking duties for the actual interaction or generated content. Requirements differ by activity and role.

Where high-risk deployer rules apply

Assess Article 26: instructions for use; competent, trained and authorised human oversight; input-data controls where relevant and under your control; monitoring; logs under your control; escalation and relevant notifications. Map each applicable duty to an owner and operating procedure. Check retention rules against the current law and data-protection requirements.

Fundamental-rights and data-protection assessments

Assess Article 27 for the specified high-risk uses and deployers, including its exceptions. A public mission does not make every AI use subject to FRIA. Where required, complete the assessment before deployment and follow notification/update requirements. Evaluate a DPIA separately under the applicable data-protection regime; one assessment does not automatically replace the other.

Where provider rules apply

For high-risk AI-system providers, assess the applicable Articles 9–15 requirements and provider duties, including documentation, quality management, conformity assessment, registration and post-market monitoring. Check the procedure for your system. For GPAI model providers, assess Articles 53 onward and systemic-risk provisions where relevant; ordinary downstream use is not automatically model provision.

Working evidence

Instructions; oversight appointment and intervention test; logging design; assessment records; disclosure samples; escalation protocol; supplier documentation. Record which obligations are applicable and which are not, with reasons.

03 / The six-dimension evidence review

The UberConsul Resilience Audit is an advisory framework, not six statutory AI Act categories. Use it to connect legal readiness with the institution’s ability to operate and defend its decisions.

Governance

Produce an accountability map: owner, controller where relevant, override authority, approvals and escalation. Test who acts when the usual decision-maker is unavailable.

Data lineage

Record training, fine-tuning, retrieval and prompt context as relevant. Identify provenance, access controls and reproducibility limits; do not claim access to vendor information you do not possess.

Model risk

Name failure modes, performance and harm signals, thresholds, monitoring frequency and the human action each threshold triggers. Test whether people can actually intervene.

Third-party dependencies

Inventory suppliers, subprocessors, models and critical integrations. Review evidence access, incident support, change notices, exit rights and substitutability.

Sovereign infrastructure

Map hosting, access, key control, jurisdictions and foreseeable compelled disclosure or interruption. Regional hosting alone does not prove sovereignty. Assess GDPR or Regulation 2018/1725 transfer rules as applicable.

Recovery posture

Document fallback operations, a substitution window and named responders. Exercise a lost-provider or model-withdrawal scenario and preserve the results.

NIS2 and DORA have separate scopes. Do not label them universal obligations for EU institutions; establish entity and sector applicability.

04 / Evidence register and official sources

A register your institution can maintain

For each requirement keep: system ID; role; article and legal version; applicable date; obligation or justified non-applicability; evidence reference; accountable owner; evidence status; unresolved gap; action; reviewer; next review date. Use restricted references instead of copying sensitive records into public tools.

Before approving a deployment

Resolve prohibited-use concerns; confirm classification and legal gates; finish required assessments; obtain required provider evidence; test oversight and fallback; confirm notices and escalation; record the accountable decision. A missing document is a gap to resolve, not an automatic compliance finding.

Official primary sources

AI Act record, versions and related acts · EUR-Lex
EDPS · Artificial Intelligence Act
Regulation (EU) 2018/1725 · EU institutional data protection
Commission · Navigating the AI Act
Commission · AI literacy questions and answers

Commission explanations are supporting guidance, not substitutes for legislation or judicial interpretation. Official web pages can change. Verify the source date and current legal text when making a decision.

Framework and next step

Kotitsas, V. (2026). The UberConsul Resilience Audit: Framework v1. UberConsul, Frankfurt am Main.
uberconsul.com/methodology
Six-dimension governance self-assessment
Book a time with UberConsul