DataDiwan

A DATADIWAN FIELD GUIDE

EU AI Act Readiness Scorecard

Score your AI system against what an EU auditor will actually ask — before you ship, not after.

Helsinki · 2026 · العربية · English · Suomi

Why this exists

Before you launch an AI feature in the EU you need to know your risk tier, what data you process, who is accountable, and what you can show an auditor. Documentation beats panic — and it starts before production. Work through the 25 checks below, tick what you can defend today, and read your score on the last page.

WHAT'S AT STAKE

Up to €35M or 7%

of global annual turnover — the EU AI Act's maximum penalty. Obligations phase in across 2025–2027. "We use the vendor's compliance" is not a defence: you remain the data controller.

WHO THIS IS FOR

Product owners, CTOs & compliance leads shipping customer chatbots, automated decision support, or internal copilots that touch personal data — in Finland, the EU, or sold to EU clients from abroad.

01 Classify the use case

Regulators look at impact, not intent.

- [ ] We have written down the single worst realistic failure mode.
  One plain sentence — "if this is wrong, X happens to Y."
- [ ] We checked whether it touches employment, credit, insurance, or essential services.
  Any "yes" points to the high-risk tier.
- [ ] A provisional risk tier is assigned — and "unsure" is treated as high-risk.
  Documented, with a date and an owner.
- [ ] Public-facing chatbots have their transparency duties noted.
  Lower tier, but never zero obligations.

Section score: ____ / 4

02 Map the data — GDPR first

You cannot be AI Act-ready without GDPR hygiene.

- [ ] A lawful basis for processing is documented.
  Consent, contract, or legitimate interest — named, not assumed.
- [ ] Data minimisation: only what retrieval needs is embedded or stored.
  No "ingest everything just in case."
- [ ] Retention limits for prompts and logs are defined.
  A number of days, enforced — not "forever."
- [ ] Transfer tools are in place for non-EU LLMs (SCCs, adequacy, or EU hosting).
  US-hosted models need a documented transfer basis.
- [ ] A DPIA exists where profiling or sensitive data is involved.
  Completed before launch, not retro-fitted.
- [ ] For RAG: indexed collections and who can query them are documented.
  Source list + access map, kept current.

Section score: ____ / 6

03 Build the audit packet

A folder an auditor can open in ten minutes.

- [ ] System card: purpose, owner, version, deployment date.
  One named human owner — not “the tech team.”
- [ ] Model card: base model, fine-tuning, temperature limits, refusal rules.
  Enough for someone to reproduce behaviour.
- [ ] Data card: sources, PII handling, deletion process.
  Maps to your GDPR records.
- [ ] Human oversight: who reviews edge cases and the escalation path.
  A name and a route, not a principle.
- [ ] Test log: red-team prompts, accuracy samples, known failure modes.
  Dated evidence you actually tested.
- [ ] Incident plan for leaks or hallucinations in production.
  Who is paged, what is said, how it's fixed.

Section score: ____ / 6

04 Transparency for users

Language accessibility is part of trust, not an afterthought.

- [ ] AI-generated content is clearly labelled.
  Visible to the user, not buried in terms.
- [ ] A human contact route is provided.
  A real inbox or person, reachable.
- [ ] Limitations are stated — “may be incomplete; verify critical decisions.”
  Plain language, near the output.
- [ ] An opt-out is offered where required.
  And it actually works.
- [ ] Key user-facing information is available in the user's language.
  Arabic / Finnish where you serve those users.

Section score: ____ / 5

05 Monitor after launch

Compliance is not a PDF on launch day.

- [ ] Prompts and outcomes are logged with retention limits.
  Enough to investigate, no more.
- [ ] The override / correction rate is tracked.
  You know how often humans fix the AI.
- [ ] Quarterly review; new features trigger re-classification.
  On the calendar, with an owner.
- [ ] RAG is re-ingested when policies change.
  Stale retrieval is itself a compliance risk.

Section score: ____ / 4

Read your score

Count every box you can defend with evidence today. Out of 25: ____ / 25

0 25

0–11	At risk	Gaps an auditor would find quickly. Start with classification and a named owner — this week.
12–18	Developing	The bones are there. Tighten data mapping, retention, and the audit packet before you scale.
19–25	Ready	Strong posture. Keep it alive with quarterly review and re-ingestion as policies move.

Want this done with you, not just read?

DataDiwan aligns AI delivery with GDPR-by-design and EU AI Act expectations — classification, documentation templates, and deployment patterns for European and cross-border teams. A focused 1–3 week sprint covers a single use case end to end.

Book a compliance-aware scoping call →

datadiwan.com