COMPLIANCE BRIEFING

Does my company really have to do nothing about AI?

A short, honest overview of which obligations actually apply when a company uses AI — and which don't. Meant as guidance, not a sales pitch.

The EU AI Act bans no company from using ChatGPT, Copilot & co., and simple, everyday AI use carries few mandatory product obligations. **But "nothing at all" is wrong.** Three duties apply across every company — and the GDPR applies anyway, from the very first record.

What actually applies

OBLIGATION	WHO	WHEN	WHAT IT MEANS
GDPR Data protection	Every company processing personal data	always	Employees who put customer or personal data into an unapproved AI tool process it with no legal basis, no data-processing agreement and no record.
AI Act · Art. 4 AI literacy	Everyone who uses AI — no exception	since 02 Feb 2025	Staff must have sufficient AI literacy — a basic grasp of the opportunities and risks of the tools they use.
AI Act · Art. 5 Prohibitions	Everyone	since 02 Feb 2025	Certain practices are banned — e.g. emotion recognition in the workplace or social scoring.
AI Act · Art. 50 Transparency	Anyone running chatbots or publishing AI content	from 02 Aug 2026	Label chatbots as AI; visibly mark AI-generated or AI-edited content.
AI Act · High-risk Annex III	Only for a high-risk use case	from 02 Dec 2027	Human oversight, logging, informing affected people. Triggered e.g. by AI in recruiting (see below).
Confidentiality Professional & contract law	Firms under client or contractual confidentiality	always	Putting client or customer data into an AI tool can breach confidentiality and trade-secret obligations — independent of the GDPR.

The AI Act has transition periods. The GDPR does not.

It applies to every processing of personal data — from the moment someone copies a customer name, an email address or a contract into an AI tool. This is the duty that hits every company immediately — regardless of size, industry or AI-Act risk tier.

The usual trigger isn't the regulator, but the first customer or auditor who asks for evidence.

High-risk — for whom, really

Broadly affected

HR & worker management. Recruiting and CV screening, but also promotion, task allocation and performance monitoring of employees.

Industry-specific

Creditworthiness (anyone assessing credit or lending) and insurance pricing (life / health).

Not high-risk

Support chatbots and lead qualification — only the transparency duty (Art. 50) applies here, not the high-risk regime.

From 02 Dec 2027 — what applies then

02 Dec 2027 doesn't suddenly make every company high-risk. But from then on the deployer duties for high-risk AI are live — and the most common way to slip into that category is AI in HR: recruiting, promotion, task allocation or performance monitoring.

The heaviest part (the conformity assessment) sits with the tool's provider; a company using AI there becomes a high-risk deployer and must then, operationally:

- **Ensure human oversight** — a competent person supervises the system.
- **Follow the instructions** — run the system as the provider specifies, not off-purpose.
- **Monitor operation** and suspend it on anomalies.
- **Keep logs ≥ 6 months** — the automatically generated records.
- **Inform affected people** when AI co-decides about them.
- **Inform employees & works council** before workplace deployment.

In practice, from an operator's view — the same duties map onto three views in Qadar AI Shield:

Which AI tools are in use — and with what data?

Discovery

Govern or block AI company-wide, monitor operation and suspend on anomalies.

Policies

Log and evidence usage — records kept for at least 6 months.

Audit Log

What this means in practice

For most companies the question isn't "Are we regulated?" but: Do we know which AI tools our team uses — and with what data? And could we prove it if someone asked? Usually the honest answer is no.

That gap — real-time visibility, policy enforcement and an audit log over AI usage — is exactly what Qadar AI closes. Not because a law forces it, but because you can't control what you can't see.

Qadar AI Limited · DIFC, Dubai
www.qadar.ai · info@qadar.ai

This document is for guidance and is not legal advice. Regulatory statements as of July 2026, EU AI Act as amended by the Digital Omnibus (adopted; publication in the EU Official Journal pending at the time of writing). Deadlines may change. Seek legal counsel for a binding assessment of your specific case.