

Shadow AI: 5-Point Instant Check

Shadow AI does not come from bad intent. It comes from a leadership vacuum. Work through these five questions honestly with your leadership team. Anyone who stalls on two or more has shadow AI — and should lead before being regulated.

1

Tools & DPAs — Which AI tools do we process data with, and is there a vetted data processing agreement in place for every one of them?

GDPR Art. 28 · fines up to €20m / 4% of turnover

2

Data & Legal Basis — Which personal or confidential data currently ends up in external AI models — and on what legal basis?

GDPR Art. 6 & Art. 5 (confidentiality)

3

Usage Policy — Is there an AI usage policy (one page is enough) that states clearly what may go in and what may not?

Basis for demonstrable due diligence & AI literacy (EU AI Act Art. 4)

4

Agents & Oversight — Do we know which automated AI workflows are running — documented, with named human oversight?

EU AI Act Art. 13/14 · fines up to €15m / 3% of turnover

5

Incident Response — Could we report a personal data breach within 72 hours, on time? And who is accountable?

GDPR Art. 33/34

Responsibility is not a value. It is a practice. Shadow AI does not disappear through bans, but through a leadership decision: what AI is meant to serve — and which guardrails apply.

Next step: 30-Minute AI Orientation · justgrow.eu

This check is not legal advice. For a binding assessment, a lawyer or data protection officer belongs at the table. © 2026 JUSTGROW