DATA SHEET

BLACKFOG®

ADX Vision

Preparing For The EU AI Act

How BlackFog ADX Vision supports compliance with the world's first comprehensive AI regulation.

[EFFECTIVE 2 AUGUST 2026]

The Regulation In Brief

The EU Artificial Intelligence Act (Regulation EU 2024/1689) is the world's first comprehensive legal framework for artificial intelligence. Adopted in May 2024 and entering into force in August 2024, the Act becomes generally applicable on 2 August 2026, with most remaining obligations taking effect on that date.

- The Act applies to providers and deployers of AI systems whose output is used in the EU, including organizations based outside the EU. Penalties for non-compliance are tiered:
  - → Up to **€35 million or 7% of global annual turnover** (whichever is higher) for prohibited AI practices under Article 5.
  - → Up to **€15 million or 3% of global annual turnover** for breaches of high-risk AI system obligations, including data governance, risk management, transparency, and cybersecurity requirements.
  - → Up to **€7.5 million or 1% of global annual turnover** for supplying incorrect or misleading information to authorities.

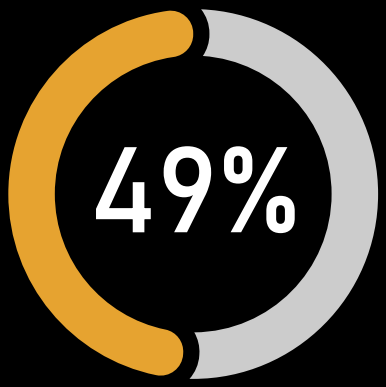
Most BlackFog customers are considered **deployers** under the Act. This includes organizations whose employees use AI systems or general-purpose AI models such as ChatGPT, Claude, Gemini, and Copilot. Deployer obligations apply regardless of whether the AI system was developed internally or accessed through a third-party provider.

The Data Exfiltration Dimension Of AI Compliance

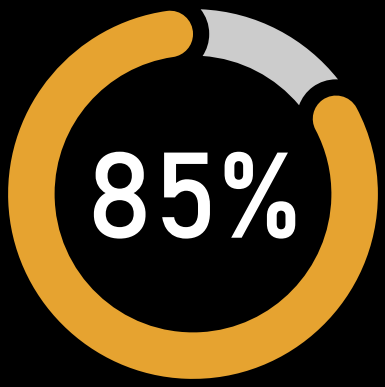
The EU AI Act sits alongside existing data protection regulations (GDPR, particularly Article 5 on data minimization and Article 32 on security of processing) and creates a converging compliance environment for any organization whose employees interact with AI tools.

The compliance challenge is structural: **employees use AI faster than security teams can govern it**.

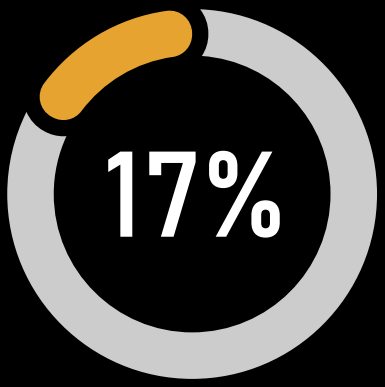
Recent BlackFog/Sapio research found:



49% of employees at companies with 500+ staff regularly paste corporate data into unapproved AI tools.



85% continue using unapproved AI tools even when sanctioned alternatives exist.



Only **17%** of organizations have technical controls in place to prevent it.

For deployers under the AI Act, this represents specific, documentable compliance exposure across multiple obligation categories.

How ADX Vision Supports EU AI Act Compliance

ADX Vision is an on-device anti data exfiltration purpose-built for the AI era. The platform supports compliance with EU AI Act obligations across four areas:

1. AI System Inventory And Mapping (Pre-2 August 2026 Requirement)

OBLIGATION:

Organizations must identify and classify AI systems in use across the enterprise, including those used by employees without formal IT approval to determine their role (provider/deployer) and risk classification.

ADX VISION CAPABILITY:

Continuous discovery of AI tool usage at the endpoint level, including ChatGPT, Claude, Gemini, Copilot, Perplexity, and other frontier model interfaces. Visibility extends to managed and unmanaged browsers, embedded AI inside SaaS applications, and personal devices on corporate networks.

2. Data Governance And Risk Management (Article 10, Article 9)

OBLIGATION:

High-risk AI deployers must implement appropriate data governance practices, including controls over training data, input data, and the protection of confidential information processed by AI systems.

ADX VISION CAPABILITY:

Real-time prevention of sensitive data flowing to AI endpoints, with policy enforcement at the prompt level. Prevents personal data, confidential business information, source code, and regulated data categories (PHI, PII, financial records) from reaching AI tools that fall outside organizational governance.

3. Transparency, Logging, And Audit Trail (Article 12, Article 13)

OBLIGATION:

Deployers must maintain logs of AI system usage and be able to demonstrate compliance to competent authorities upon request.

ADX VISION CAPABILITY:

Detailed audit trails of every AI interaction at the endpoint, which user, which AI tool, what data category, what policy outcome. Exportable to existing compliance reporting systems. Supports the documentation requirements under Article 12 and the response-to-authorities requirements under Article 21.

4. AI Literacy And Workforce Controls (Article 4, In Force Since February 2025)

OBLIGATION:

Providers and deployers must ensure that staff who deal with AI systems have a sufficient level of AI literacy. This obligation has been legally enforceable since 2 February 2025.

ADX VISION CAPABILITY:

Real-time policy notifications inform organizations when actions trigger AI governance rules, creating an opportunity for additional training that complements formal AI literacy programs. Activity logs surface gaps in policy understanding for targeted intervention.

Why Endpoint-Native Architecture Matters For AI Act Compliance

The Act's requirements apply regardless of how employees access AI. This creates a coverage problem for security architectures that depend on a specific channel:

- **Network-layer tools (CASB, SWG)** cannot decrypt conversational data in browser sessions to legitimate LLM domains.
- **Browser extensions** only work on managed browsers; they miss personal devices, unmanaged endpoints, and embedded AI inside approved SaaS.
- **API gateways** only see sanctioned enterprise AI deployments; they miss the consumer tools that drive most shadow AI risk.

ADX Vision's endpoint-native architecture sees AI activity across managed and unmanaged browsers, embedded AI inside SaaS, personal devices on corporate networks, offline and air-gapped environments, and emerging autonomous AI agents. For deployers, this is the only architecture that supports complete documentation of AI usage across the enterprise.

Implementation Timeline

ADX Vision deploys as a lightweight endpoint agent on Windows and macOS, with a centralized BlackFog Console. Typical enterprise deployment timelines:

- **Days 1-7:** Agent deployment, console configuration, baseline AI usage discovery.
- **Days 8-30:** Policy framework definition aligned to EU AI Act obligations.
- **Days 31-90:** Policy enforcement rollout, audit trail validation, compliance reporting templates established.

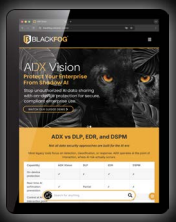
Organizations beginning deployment in Q2 2026 can be operational ahead of the 2 August 2026 enforcement date.

Next Steps

Request a Demo: See how **ADX Vision** discovers and governs AI usage in your environment. Start the DPIA Assessment: Identify hidden AI exfiltration risks across your endpoints.

BlackFog Inc. Source: Regulation (EU) 2024/1689 (Artificial Intelligence Act) and supporting Commission guidance through 2026. This datasheet is provided for informational purposes and does not constitute legal advice.

ADX Vision
Useful Resources



Product Page

FIND OUT MORE

Video Overview

WATCH

Blog

READ

Console

DEMO

Datasheet

DOWNLOAD

Follow Us

Award-winning Technology

Contact us for a demo

Start your free trial

Visit blackfog.com