Gruppo BitAgorà Smart Network

Responsabilità per danni da IA

Cosa cambia per le aziende italiane con il decreto attuativo dell'AI Act europeo. Avere uno strumento AI certificato **non mette al riparo da nulla**.

Due principi fondamentali

La conformità non esclude la responsabilità

Un sistema AI conforme all'AI Act non copre i danni prodotti nel contesto aziendale specifico. Quello che accade con i tuoi dati e processi rimane responsabilità tua.

Onere della prova alleggerito

Chi subisce un danno da un sistema AI ha più strumenti per dimostrare il nesso causale, senza dover ricostruire da solo l'intera catena tecnica. Si abbassa la soglia di accesso alla tutela legale.

Gruppo BitAgorà Smart Network

Provider vs Deployer

L'AI Act distingue due figure chiave: il **provider** (chi sviluppa e immette sul mercato il sistema AI) e il **deployer** (chi lo usa in contesto operativo). Per le PMI italiane, la figura di riferimento è quasi sempre quella del **deployer**.

Gli obblighi del Deployer

Uso corretto

Seguire le istruzioni del provider

Dati pertinenti

Garantire la qualità degli input

Supervisione umana

Assicurare un controllo adeguato

Non serve costruire un algoritmo proprietario per essere deployer di un sistema AI ad alto rischio.

Già deployer senza saperlo

I software aziendali più comuni includono già moduli AI che possono rientrare nella categoria **ad alto rischio** dell'AI Act:

Software HR

Gestionali con moduli di analisi del personale

Scoring creditizio

Sistemi di analisi finanziaria automatizzata

Assistenza clienti

Piattaforme con decisioni automatiche

Sicurezza informatica

Sistemi che classificano incidenti automaticamente

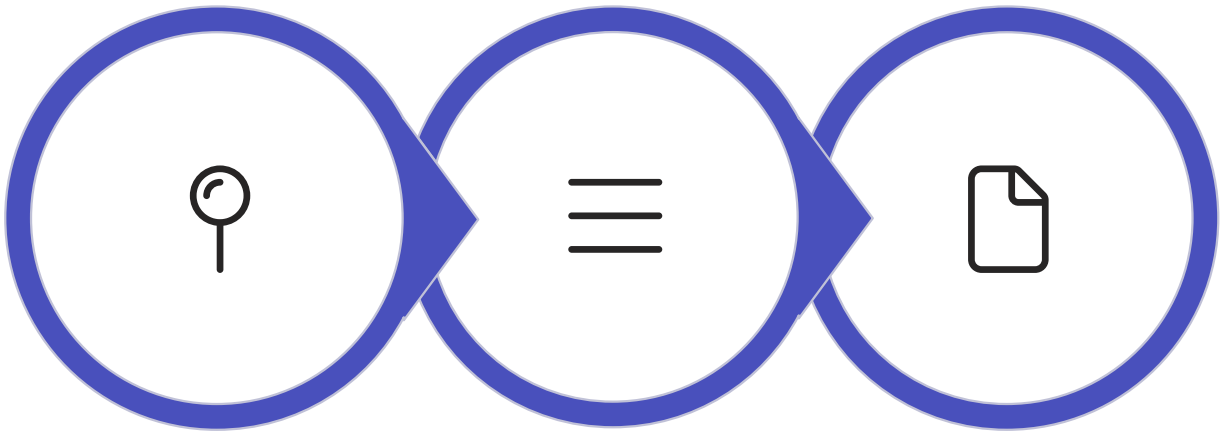
Strumenti AI a rischio: selezione del personale

Cosa rientra nell'alto rischio

Gli strumenti che **analizzano CV o video-colloqui** per supportare decisioni di assunzione sono esplicitamente classificati come sistemi AI ad alto rischio dall'AI Act.

Se la tua azienda usa software di recruiting con funzionalità AI, sei già un deployer soggetto agli obblighi normativi.

Tre azioni concrete da fare adesso



Mappare strumenti

Verificare documenti

Supervisione umana

Queste tre azioni costituiscono la base minima per gestire il rischio legale e dimostrare diligenza in caso di contestazione.

Passo 1 — Mappare gli strumenti AI

Cosa fare

Identificare tutti i software in uso che includono funzionalità AI in grado di influenzare **decisioni su persone o processi critici**: HR, finanza, customer service, sicurezza.

> ⚠ Non limitarsi agli strumenti dichiaratamente "AI": molti gestionali includono moduli automatizzati non etichettati come tali.

Obiettivo

Avere una mappa chiara di quali sistemi rientrano nell'ambito dell'AI Act e quali obblighi comportano per il deployer.

Passi 2 e 3 — Documentazione e supervisione

1

Verificare la documentazione del provider

Per ogni strumento a rischio, il provider deve fornire: documentazione tecnica, istruzioni d'uso e indicazioni sulla supervisione umana. Richiederla e conservarla.

2

Strutturare la supervisione umana

Documentare **chi supervisiona cosa e in quale formato**. Questa documentazione è la prima difesa in caso di contestazione legale.

Inizia oggi

Le regole ci sono già. La responsabilità è già attiva. La conformità all'AI Act non ti protegge automaticamente: serve una gestione consapevole e documentata dell'IA in azienda.

Per approfondire e ricevere supporto: **bitagora.it/contatti**