AVVERA

SB
Società Benefit

GUIDA OPERATIVA

AI ACT IN AZIENDA

SOMMARIO

INTRODUZIONE

L'**Artificial Intelligence Act (AI Act)** è il primo regolamento al mondo sull'uso dell'intelligenza artificiale. Entra in vigore gradualmente a partire dal 2024–2026 e stabilisce obblighi diversi in base al **rischio** dei sistemi AI.

Questa dispensa è pensata per i nostri clienti come un "regalo di Natale" di valore: una **guida pratica**, comprensibile, e immediatamente applicabile nell'organizzazione.

Obiettivi:

- comprendere *cosa richiede l'AI Act*;
- identificare *dove l'azienda utilizza l'AI* (anche "nascosta");
- classificare i sistemi AI per livello di rischio;
- adottare checklist operative e modelli documentali.

L'AI ACT IN SINTESI

A chi si applica

Si applica a:

- fornitori di sistemi IA (chi li sviluppa o li commercializza);
- deployer/ utilizzatori (le aziende che li implementano);
- importatori, distributori, integratori.

Punti chiave

- Si applica anche all'AI sviluppata fuori dall'UE ma utilizzata nell'UE.
- Prevede un approccio risk-based.

GLI OBIETTIVI DELL'AI ACT

L'AI Act nasce con l'ambizione dichiarata di creare **il primo quadro normativo organico al mondo per regolare l'intelligenza artificiale**, con un equilibrio complesso: promuovere l'innovazione e proteggere i diritti fondamentali.
Per comprenderne la logica — e per applicarlo correttamente in azienda — è fondamentale cogliere le finalità che hanno guidato il legislatore europeo.

Tutelare i diritti fondamentali e i valori dell'UE

L'obiettivo primario è garantire che l'AI sia sviluppata e utilizzata in modo da **preservare i diritti delle persone**, in particolare:

- diritto alla non discriminazione;
- protezione dei dati personali;
- dignità umana;
- libertà di espressione e informazione;
- libertà professionale e diritto al lavoro;
- tutela dei consumatori.

Traduzione operativa in azienda

- introdurre controlli su bias e discriminazioni;
- fornire trasparenza su modelli e decisioni automatizzate;
- garantire sempre una supervisione umana nei casi critici.

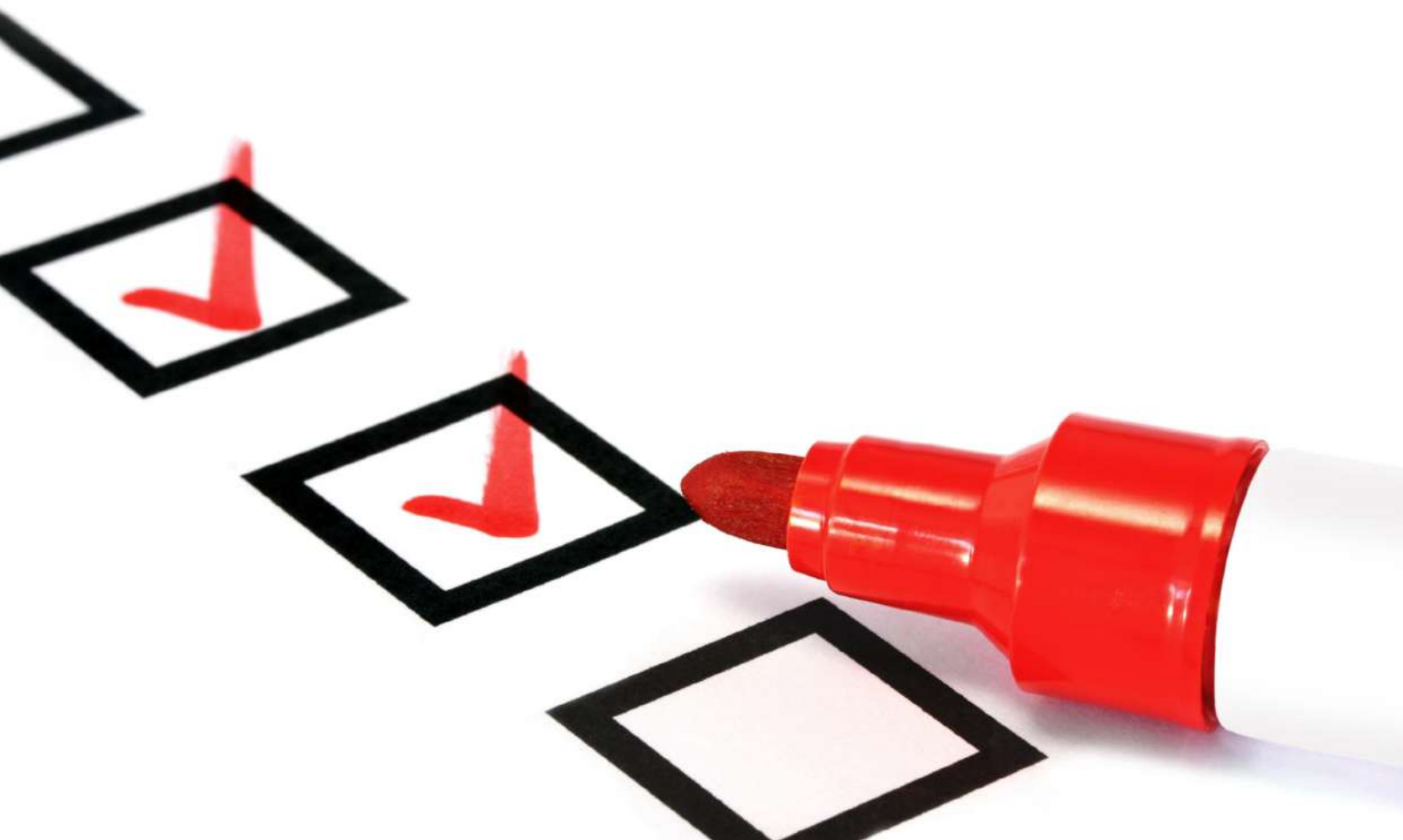
RAFFORZARE LA SICUREZZA DEI SISTEMI AI

L'AI Act mira a prevenire rischi legati a:

- malfunzionamenti;
- vulnerabilità cybersecurity;
- manipolazioni intenzionali;
- effetti imprevedibili dei modelli.

Traduzione operativa

- logging e tracciabilità;
- stress test periodici;
- audit tecnici;
- requisiti di robustezza e resilienza.



CREARE FIDUCIA NELL'ADOZIONE DELL'AI

La percezione di rischio, opacità o imprevedibilità dell'AI rischia di ostacolare l'innovazione. L'AI Act vuole creare **un ambiente di fiducia**, affinché cittadini e imprese possano usare l'AI senza timori.

Traduzione operativa

- informative chiare;
- governance interna ben definita;
- certificazioni e conformità verificabile;
- processi documentati per ogni sistema AI.

PROMUOVERE L'INNOVAZIONE E LA COMPETITIVITÀ DELL'UE

L'obiettivo non è affatto "frenare l'AI". Al contrario, il regolamento:

- crea un quadro stabile e prevedibile per gli investimenti;
- introduce sandbox normative per sperimentare in sicurezza;
- riduce i rischi legali per le aziende che adottano processi di conformità.

Traduzione operativa

- possibilità di partecipare a sandbox regolatorie;
- utilizzo della compliance come elemento competitivo e di branding;
- sviluppo di AI interne con criteri "by design" conformi al mercato.

Armonizzare il quadro normativo europeo

L'AI Act evita la frammentazione regolatoria tra Stati Membri, garantendo un **mercato unico dell'AI**, con regole condivise per:

- fornitori;
- integratori;
- utilizzatori;
- distributori;
- modelli generici (GPAI).

Traduzione operativa

- semplificazione per le aziende multinazionali;
- possibilità di utilizzare sistemi AI uniformemente in tutti i paesi UE;
- riduzione dei costi di compliance multipaese.

Prevenire usi distorti o abusivi dell'AI

L'AI Act individua categorie vietate per contrastare:

- sorveglianza massiva;
- manipolazione subliminale;
- social scoring;
- sfruttamento delle vulnerabilità.

Traduzione operativa

- valutare attentamente casi d'uso borderline;
- predisporre un comitato etico interno per l'approvazione dei casi d'uso;
- documentare motivazioni e controlli per gli utilizzi ad alto impatto.

GARANTIRE TRASPARENZA E RESPONSABILITÀ

L'obiettivo è assicurare che:

- le aziende sappiano cosa fa il sistema AI;
- i cittadini possano essere informati adeguatamente;
- le decisioni critiche non siano "scatole nere".

Traduzione operativa

- definizione di accountability interna;
- policy che definiscono ruoli e responsabilità;
- strumenti di explainability e reporting.

CLASSIFICAZIONE DEI RISCHI

A. Rischio Inaccettabile (vietato)

- social scoring generalizzato;
- manipolazione subliminale;
- sfruttamento delle vulnerabilità;
- riconoscimento biometrico in tempo reale in spazi pubblici (salvo eccezioni);
- biometria ex -post su larga scala;
- database biometrici tramite scraping massivo;
- categorizzazione biometrica su caratteristiche sensibili;
- emotion recognition nelle scuole e sul lavoro;
- polizia predittiva basata su profiling;
- manipolazione politica di gruppi elettorali.

Esito: divieto assoluto.

Questi divieti sono già pienamente in vigore e immediatamente applicabili.

B. Alto Rischio (High-Risk)

Due categorie:

- AI come componente di sicurezza (es. robotica industriale, dispositivi medici).
- AI impiegata in settori critici:
  - HR e selezione del personale;
  - valutazione creditizia;
  - gestione infrastrutture critiche;
  - giustizia e law enforcement;
  - educazione e formazione professionale;
  - accesso e valutazione di servizi essenziali e pubblici;

- migrazione, asilo e controllo delle frontiere;
- amministrazione della giustizia e processi democratici.

Cosa NON è High-Risk (chiarimenti utili per le aziende)

Non rientrano automaticamente nel rischio alto:

- chatbot generativi → rischio limitato;
- strumenti di marketing predittivo → basso/medio rischio;
- sistemi di automazione generica;
- AI che assiste ma non decide in modo significativo.

La soglia *determinante è se l'AI influisce significativamente su diritti, accesso a servizi o sicurezza fisica.*

Esito: forti obblighi di compliance.

Gli obblighi relativi a questa categoria entreranno in vigore dal 2 agosto 2026 (salve diverse disposizioni normative)

C. Rischio Limitato

I sistemi a rischio limitato sono quei sistemi di AI che non hanno impatti significativi sulla sicurezza o sui diritti fondamentali, ma possono generare rischi legati a trasparenza, comprensione dell'utente o potenziali manipolazioni

Esempio:

Sistemi che interagiscono con l'utente (es. chatbot, assistenti virtuali sui siti web, tool LLM che rispondono automaticamente ai clienti, generatori di deepfake non fraudolenti, ecc).

*Esito: Obblighi di trasparenza - l'utente deve sapere **chiaramente** e **prima dell'interazione** che sta interagendo con un sistema di AI.*

Gli obblighi dei sistemi Limited-Risk sono già pienamente in vigore (Art. 50–52).

SISTEMI A RISCHIO LIMITATO — COSA FARE SUBITO (Art. 50–52)

- Dichiarare che l'utente interagisce con un AI
- Etichettare contenuti generati, modificati o sintetici
- Garantire che l'utente possa comprenderlo facilmente
- Usare interfacce trasparenti (no dark patterns)
- Formare il personale sul corretto uso dei tool AI generativi

D. Rischio Minimo

I **sistemi a rischio minimo** costituiscono la categoria più ampia dell'AI Act.

Comprendono la maggior parte degli usi aziendali "ordinari" dell'intelligenza artificiale che **non incidono sui diritti fondamentali** e **non comportano rischi significativi per la sicurezza**.

Esempi tipici:

- strumenti di AI incorporati nel software comune (es. funzioni intelligenti in produttività office);
- modelli per analytics non utilizzati per decisioni su persone;
- sistemi di clustering, segmentazione o forecasting non impattanti su diritti;
- filtri antispam;
- suggerimenti automatici non decisivi (es. "auto-complete");
- sistemi generativi usati solo per brainstorming o creatività interna.

Per questi sistemi non ci sono obblighi specifici né vincoli di conformità.

Rischio minimo ≠ rischio trascurabile

Anche se non vi sono obblighi formali, l'azienda dovrebbe:

- evitare un uso "non controllato" che possa sconfinare in processi sensibili;
- valutare periodicamente se cambiano finalità o perimetro d'uso;
- mantenere un livello basico di tracciabilità.

OBBLIGHI PER LE AZIENDE (DEPLOYER)

Gli obblighi cambiano in funzione della **categoria di rischio del sistema AI**: *Inaccettabile, Alto, Limitato, Minimo*. L'obiettivo è guidare l'azienda a **usare l'AI in modo sicuro, trasparente e conforme**.

Di seguito uno schema sintetico e operativo.

Obblighi generali per tutte le aziende

- **Classificare tutti i sistemi AI** presenti in azienda secondo la loro categoria di rischio.
- Adottare una policy aziendale AI.
- Formare il personale sulla gestione dei rischi.
- Stabilire un *AI Governance Team* (o esternalizzarlo).

Obblighi specifici per categoria di rischio

Categoria	Obblighi principali	Note operative
Inaccettabile	- Vietati	Nessun uso consentito; sanzioni immediate se utilizzati
Alto Rischio	- Documentazione tecnica completa (Art. 8–11) - Valutazione AI Impact Assessment (AIA) - Gestione rischio e mitigazioni - Registrazione UE dei sistemi - Logging e audit - Human oversight	Applicazione obbligatoria; integratori devono garantire compliance completa
Rischio Limitato	- Trasparenza verso utenti (Art. 50–52) - Disclosure di contenuti generati o sintetici - Interfacce chiare e comprensibili	Obblighi già in vigore; focus su comunicazione chiara e correttezza dei contenuti
Rischio Minimo	- Nessun obbligo legale specifico	Buone pratiche: mappare sistemi, monitorare evoluzioni, formazione base del personale

Rischio Inaccettabile

- Uso vietato (Art. 5).
- Sistemi come social scoring per bonus/penalità, sorveglianza biometrica in tempo reale in luoghi pubblici, AI manipolativa subliminale.
- Già in vigore: qualsiasi utilizzo comporta sanzioni immediate.

Alto Rischio

- Obblighi dettagliati (Art. 6–15, Allegato III):
  - Documentazione tecnica completa (architettura, dati, limiti).
  - Valutazione del rischio (AI Impact Assessment).
  - Logging, audit e tracciabilità delle decisioni.
  - Supervisione umana (human oversight).
  - Registrazione dei sistemi in un database UE.
  - Esempi: screening CV automatico, scoring creditizio, sistemi sanitari, infrastrutture critiche.

Rischio Limitato

- Obblighi principali (Art. 50–52):
  - Trasparenza verso gli utenti: comunicare che si sta interagendo con un AI.
  - Disclosure dei contenuti generati o sintetici.
  - Interfacce chiare e comprensibili.
  - Esempi: chatbot generativi, LLM per supporto redazionale, sistemi di raccomandazione.

Rischio Minimo

- Nessun obbligo legale specifico (Art. 2, Considerandi 70–72).
- Buone pratiche consigliate: mappare i sistemi, monitorarne l'evoluzione, formare il personale.
- Esempi: strumenti di produttività office, analisi interne non decisionali, filtri antispam.

OBBLIGHI PER L'USO DI MODELLI GPAI / FOUNDATION MODELS

Quando un'azienda integra modelli **general purpose AI (GPAI)**:

- **Verificare la documentazione fornita dal fornitore** (architettura, dati di addestramento, policy d'uso).
- **Valutare rischi operativi** (allucinazioni, bias, vulnerabilità).
- Garantire trasparenza verso utenti e dipendenti se il modello interagisce con persone.
- Adottare policy interne di uso responsabile.
- **Se il modello è integrato in processi critici**, classificare il sistema come High-Risk e applicare tutti gli obblighi del Capo II.

COME IDENTIFICARE L'AI IN AZIENDA

Molte aziende usano l'AI senza saperlo. L'AI Act si applica anche ai modelli integrati in software di terze parti.

Dove guardare:

- Software HR (ATS, screening CV automatizzato).
- Tool di marketing (profilazione, lead scoring).
- ERP con moduli predittivi.
- Sistemi di controllo qualità in fabbrica (vision AI).
- CRM con suggerimento next-best-action.
- Soluzioni cloud che integrano LLM (Microsoft Copilot, Google Duet, ecc.).

DEFINIZIONE OPERATIVA DI AI

Secondo l'AI Act, si considera **AI qualsiasi sistema che:**

- utilizza **algoritmi o modelli** per prendere decisioni, supportare decisioni o generare output;
- apprende dai dati (machine learning, deep learning, NLP, CV, ecc.);
- simula capacità umane (ragionamento, linguaggio, riconoscimento immagini, generazione contenuti).

Esempio: anche strumenti di previsione automatica, chatbot, generatori di contenuti o software di raccomandazione rientrano nella definizione di AI.

PASSAGGI PRATICI PER L'IDENTIFICAZIONE

1. Mappatura dei processi aziendali

- Elencare tutte le aree aziendali che usano software digitale: HR, marketing, customer care, produzione, finanza, R&D.
- Per ogni processo, chiedersi: "Viene preso qualche output decisionale o predittivo dall'AI?"

2. Inventario dei sistemi

- Registrare tutti i software, tool, piattaforme e modelli integrati.
- Includere anche strumenti cloud e SaaS, add-on, plugin o modelli integrati in applicazioni esistenti.

3. Verifica dell'uso dell'AI

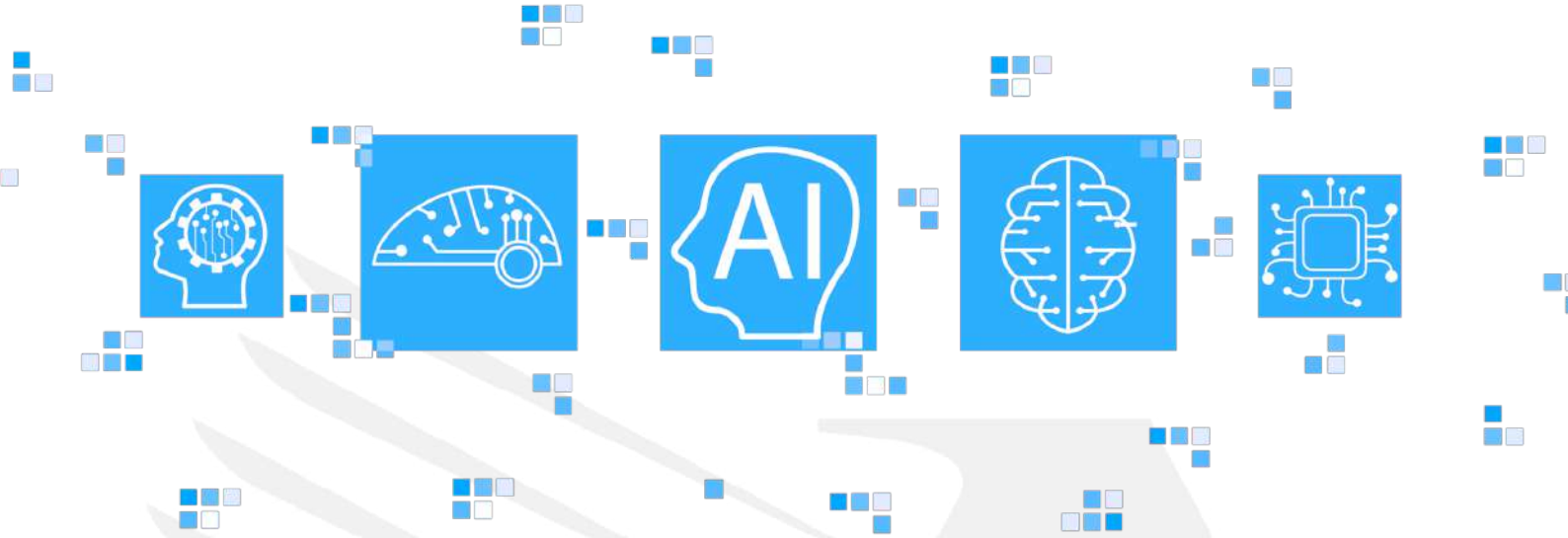
- Identificare se il software genera **output autonomi**, raccomandazioni o decisioni.
- Controllare se usa tecniche di machine learning, deep learning, NLP o modelli generativi.
- Coinvolgere team IT, sicurezza e data science per confermare la presenza di componenti AI.

4. Classificazione preliminare

- Per ciascun sistema AI identificato, fare una prima classificazione del rischio:
  - Inaccettabile, Alto, Limitato o Minimo.
- Questo aiuta a determinare i successivi obblighi normativi.

STRUMENTI PRATICI PER L'IDENTIFICAZIONE

- **Questionario interno AI** per dipartimenti e team: chiedere quali strumenti utilizzano, output generati e finalità.
- **Audit tecnico**: analizzare log, API, modelli integrati e librerie utilizzate.
- **Coinvolgimento dei fornitori**: richiedere informazioni sui sistemi AI forniti (ad esempio LLM, modelli generativi, soluzioni predictive).
- **Software di inventario IT**: integrare informazioni sull'uso di modelli AI.



BUONE PRATICHE OPERATIVE

- Documentare **tutti i sistemi identificati** in un registro AI interno.
- Aggiornare periodicamente l'inventario per includere **nuove integrazioni o aggiornamenti di modelli**.
- Creare un **responsabile interno AI** per garantire supervisione, gestione rischi e compliance.
- Collegare l'inventario alla **classificazione dei rischi** e agli obblighi normativi.

ESEMPI PRATICI PER FUNZIONE AZIENDALE

Per capire concretamente come l'AI può essere presente in azienda, è utile guardare funzione per funzione i possibili casi d'uso, con la relativa categoria di rischio e gli obblighi principali previsti dall'AI Act.

Risorse Umane (HR)

In ambito HR, l'AI viene spesso utilizzata per screening dei candidati, analisi delle performance dei dipendenti o gestione delle FAQ tramite chatbot.

- Il screening automatico dei CV è considerato un sistema ad alto rischio. Per questo motivo, richiede documentazione tecnica completa, valutazione AI Impact Assessment (AIA) e supervisione umana per ridurre il rischio di bias.
- L'analisi delle performance dei dipendenti, invece, rientra spesso nella categoria rischio limitato, con l'obbligo principale di trasparenza verso i dipendenti: essi devono sapere che i dati vengono analizzati da un sistema AI.
- I chatbot HR, usati per rispondere a domande frequenti, rientrano anch'essi in rischio limitato, con l'obbligo di informare gli utenti che stanno interagendo con un AI.

Marketing e Vendite

In marketing e vendite, l'AI supporta la personalizzazione delle campagne, la generazione automatica di contenuti e l'analisi predittiva delle vendite.

- I sistemi di raccomandazione prodotti e i chatbot di supporto marketing sono considerati a rischio limitato. Qui l'obbligo principale è garantire la trasparenza sui contenuti generati dall'AI.
- L'analisi predittiva delle vendite e gli strumenti di forecast interno rientrano invece nel rischio minimo, senza obblighi legali specifici. Tuttavia, è buona pratica monitorare i risultati e documentare l'uso del sistema.

Customer Care

Nel servizio clienti, l'AI è spesso impiegata per chatbot, analisi dei sentiment dei clienti e risposta automatica ai ticket.

- I chatbot GPT-like e simili rientrano nel rischio limitato: occorre informare sempre l'utente che sta interagendo con un sistema AI e garantire trasparenza sui contenuti generati.
- L'analisi dei sentiment dei clienti è generalmente a rischio minimo, utilizzata per migliorare il servizio senza influire su decisioni critiche.
- Anche la risposta automatica ai ticket è tipicamente a rischio minimo, ma richiede una supervisione periodica per assicurare qualità e affidabilità.

Produzione e Operations

In produzione, l'AI viene impiegata per manutenzione predittiva, ottimizzazione della logistica e robotica autonoma.

- La manutenzione predittiva o l'ottimizzazione della supply chain rientrano nel rischio minimo: non ci sono obblighi legali, ma è consigliabile monitorare costantemente i dati e aggiornare i modelli.
- La robotica autonoma con supervisione umana può essere considerata ad alto rischio, con necessità di documentazione tecnica, AIA e controllo umano per garantire la sicurezza operativa.

Finanza e Controllo

In ambito finanziario, l'AI supporta il credit scoring, la prevenzione delle frodi e l'analisi predittiva.

- I sistemi di scoring creditizio e di prevenzione frodi sono High-Risk, soggetti a tutti gli obblighi di compliance: AIA, documentazione tecnica, registrazione UE e supervisione umana.
- L'analisi predittiva dei fatturati, invece, rientra nel rischio minimo, senza obblighi specifici, pur essendo utile come strumento interno di pianificazione.

Ricerca e Sviluppo (R&D)

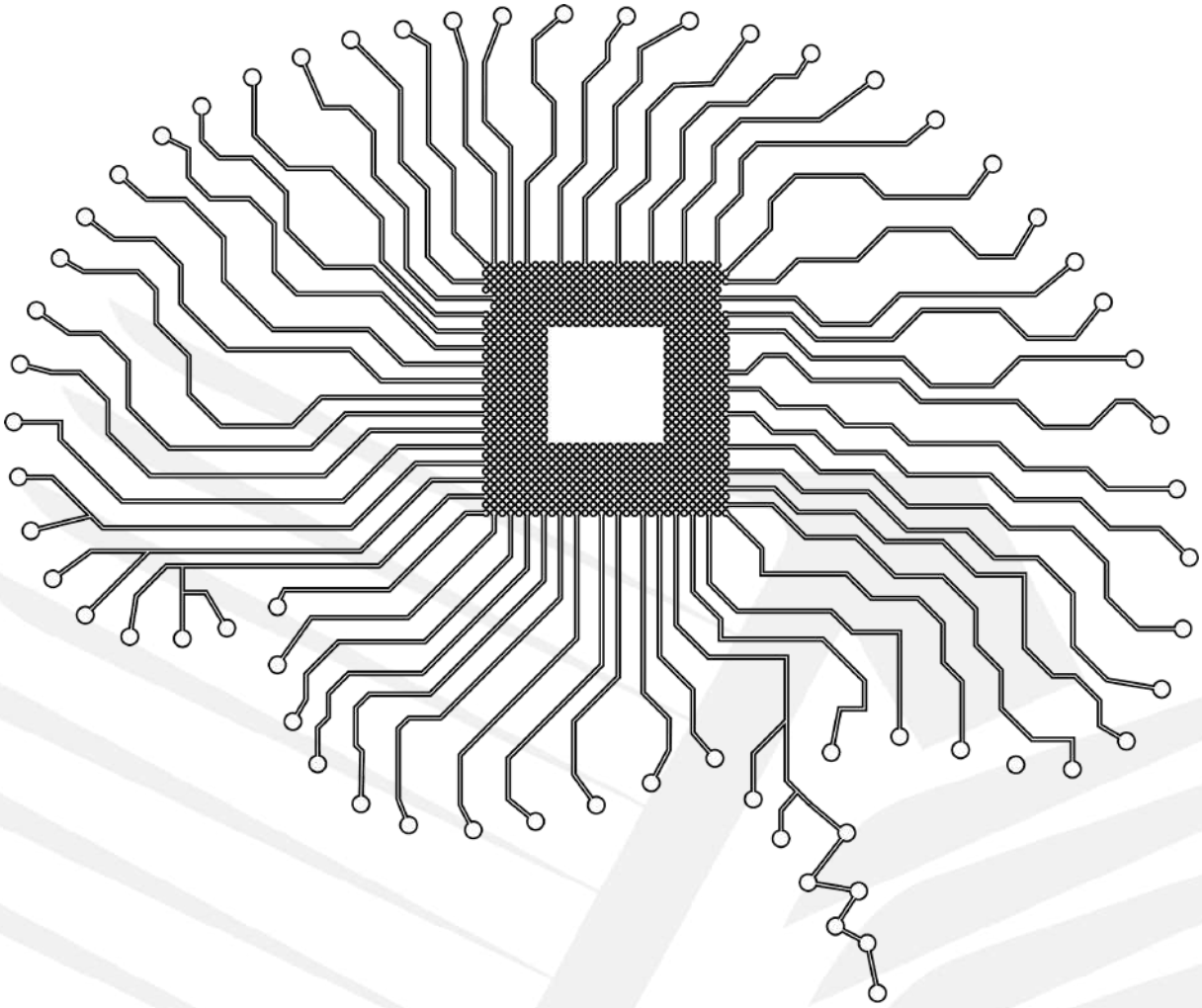
Nel reparto R&D, l'AI è spesso utilizzata per generare prototipi, simulazioni o design creativo.

- La generazione di prototipi o di design AI-generated rientra nel rischio minimo o limitato, con obblighi di trasparenza se i risultati vengono condivisi esternamente.

- Le simulazioni critiche per la sicurezza possono essere High-Risk, richiedendo documentazione tecnica e supervisione umana accurata.

Buone pratiche trasversali

- Tutti i sistemi AI devono essere mappati in un registro interno e classificati per categoria di rischio.
- È fondamentale formare il personale sull'uso responsabile dei sistemi AI.
- Occorre monitorare periodicamente le performance e i rischi, soprattutto per i sistemi generativi e quelli ad alto rischio.



CHECKLIST OPERATIVE

Checklist generale

Questa checklist raccoglie i passaggi fondamentali per garantire che i sistemi AI aziendali siano **identificati, classificati e gestiti in conformità con l'AI Act**.

Mappatura dei sistemi AI

- Identificare tutti i sistemi AI presenti in azienda, inclusi software interni, SaaS, cloud e modelli esterni.
- Coinvolgere i reparti chiave (HR, Marketing, Customer Care, Produzione, Finanza, R&D) per avere una panoramica completa.

Classificazione del rischio

- Assegnare a ciascun sistema la categoria di rischio secondo l'AI Act: Inaccettabile, High-Risk, Limited-Risk o Minimal-Risk.
- Documentare la motivazione della classificazione.

Richiesta documentazione ai fornitori

- Ottenere dettagli tecnici sui sistemi AI forniti: algoritmi, modelli utilizzati, misure di sicurezza, eventuali valutazioni di impatto già effettuate.

Valutazione d'impatto AI (AI Impact Assessment)

- Applicare l'AIA ai sistemi ad alto rischio, documentando potenziali impatti sui diritti fondamentali e le misure di mitigazione.

Definizione ruoli (AI Officer, IT, Legal, Risk Management)

- Assegnare responsabilità chiare per gestione, supervisione e compliance dei sistemi AI.
- Garantire che ogni ruolo sappia quali obblighi normativi deve rispettare.

Procedure di human oversight

- Stabilire meccanismi di supervisione umana sui sistemi High-Risk e Limited-Risk critici.
- Definire responsabilità e modalità di intervento in caso di output AI problematici.

Registro interno AI

- Creare e mantenere aggiornato un registro con:
  - Nome del sistema AI
  - Funzione aziendale associata
  - Categoria di rischio
  - Obblighi applicabili
  - Documentazione tecnica disponibile
  - Responsabile interno

Piano formazione dipendenti

- Formare il personale sull'uso responsabile dei sistemi AI, sui rischi, sugli obblighi di trasparenza e sulle procedure interne.
- Aggiornare la formazione in base all'evoluzione dei sistemi e della normativa.

Meccanismo per segnalazioni incidenti AI

- Definire procedure interne per la gestione di errori, bias o malfunzionamenti dei sistemi AI.
- Garantire canali di segnalazione chiari e accessibili a tutti i dipendenti.

CHECKLIST PER CONTRATTI CON FORNITORI AI

Questa checklist aiuta a **inserire nei contratti con fornitori di sistemi AI tutte le clausole necessarie per la compliance e la gestione dei rischi**, secondo l'AI Act.

Clausola di conformità all'AI Act

- Inserire obbligo contrattuale che il fornitore garantisca la conformità dei sistemi AI alla normativa europea.
- Prevedere che eventuali aggiornamenti normativi siano recepiti tempestivamente dal fornitore.

Accesso a log e metriche

- Garantire all'azienda il diritto di accesso ai log operativi e alle metriche dei sistemi AI.
- Assicurarsi che i dati forniti siano sufficienti per monitorare correttezza, bias e performance del modello.

Audit e test congiunti

- Prevedere la possibilità di condurre audit periodici e test congiunti dei sistemi AI.
- Stabilire modalità, frequenza e responsabilità per l'esecuzione di tali controlli.

Obbligo di notificare vulnerabilità

- Inserire clausola che obblighi il fornitore a segnalare tempestivamente eventuali vulnerabilità, malfunzionamenti o anomalie rilevate.
- Definire i tempi e le modalità di notifica e risoluzione.

SLA di sicurezza

- Definire Service Level Agreement chiari in termini di sicurezza, continuità operativa e risoluzione incidenti.
- Stabilire metriche, tempi di intervento e responsabilità per eventuali violazioni.

ALTRE CHECKLIST

Checklist per l'implementazione di nuovi sistemi AI

Questa checklist è utile **prima di introdurre un nuovo sistema AI in azienda**. Aiuta a valutare rischio, obblighi normativi e impatti operativi:

- Analisi del caso d'uso e processo aziendale coinvolto
- Classificazione del rischio AI secondo l'AI Act
- AI Impact Assessment preliminare
- Verifica di conformità normativa e regolamentare
- Definizione ruoli e responsabilità (AI Officer, IT, Legal, Risk Management)
- Pianificazione della supervisione umana (human oversight)
- Definizione di metriche e log per monitoraggio continuo
- Procedure per test, validazione e revisione periodica del modello

Checklist di monitoraggio periodico dei sistemi AI

Questa checklist serve per **audit e controllo continuo dei sistemi già operativi**, fondamentale soprattutto per High-Risk e Limited-Risk:

- Controllo aggiornamenti dei modelli e dei dataset
- Verifica correttezza, bias e affidabilità dei risultati
- Revisione dei log e delle metriche di performance
- Controllo del rispetto degli obblighi di trasparenza verso utenti e dipendenti
- Aggiornamento registro interno AI
- Valutazione necessità di AIA aggiornata per High-Risk

Checklist per la gestione degli incidenti AI

Indispensabile per garantire **risposta rapida e gestione dei rischi:**

- Identificazione e classificazione dell'incidente (errore, bias, malfunzionamento)
- Notifica interna ai responsabili (AI Officer, IT, Legal)
- Coinvolgimento del fornitore se necessario
- Documentazione dell'incidente e azioni correttive
- Comunicazione eventuale a stakeholder esterni (clienti, autorità)
- Revisione procedure e aggiornamento piani di mitigazione

Checklist per l'uso dei modelli generativi / GPAI

Data la crescente diffusione di **foundation models**, è utile avere linee guida dedicate:

- Verifica rischi potenziali di output non accurati o fuorvianti
- Obbligo di disclosure quando i contenuti sono AI-generated
- Monitoraggio per bias o contenuti inappropriati
- Definizione di limiti d'uso e supervisione umana
- Registro degli utilizzi dei modelli generativi
- Valutazione periodica dei modelli aggiornati

Checklist per la documentazione e audit esterni

- Preparazione della documentazione tecnica richiesta dall'AI Act
- Evidenziazione di misure di sicurezza, human oversight e mitigazione rischi
- Disponibilità di log e metriche per audit esterni o ispezioni
- Aggiornamento dei registri e dei report di monitoraggio

DOCUMENTAZIONE DA IMPLEMENTARE

Per garantire la **conformità all'AI Act** e la gestione efficace dei rischi, è fondamentale predisporre e mantenere aggiornata una serie di documenti interni. Questi documenti servono sia per l'**audit interno**, sia per eventuali **controlli esterni o ispezioni da parte delle autorità competenti**.

Registro dei sistemi AI

- Elenco completo di tutti i sistemi AI presenti in azienda, interni ed esterni (SaaS, cloud, modelli esterni).
- Per ogni sistema indicare:
  - Funzione aziendale
  - Categoria di rischio (High-Risk, Limited-Risk, Minimal-Risk)
  - Obblighi normativi applicabili
  - Responsabile interno
  - Versione del modello e aggiornamenti

Documentazione tecnica dei sistemi AI

- Dettagli su algoritmi, dataset utilizzati e metodologia di addestramento.
- Informazioni sul funzionamento del modello, limiti e potenziali rischi.
- Misure di sicurezza implementate e procedure di human oversight.
- Log e metriche operative necessarie per monitoraggio e audit.

AI Impact Assessment (AIA)

- Valutazioni d'impatto per tutti i sistemi High-Risk.
- Analisi dei rischi per i diritti fondamentali, bias e discriminazioni.
- Misure di mitigazione e piani d'azione per ridurre i rischi.
- Aggiornamento periodico dell'AIA, soprattutto in caso di aggiornamenti dei modelli o cambiamenti del processo aziendale.

Contratti e accordi con fornitori di AI

- Clausole di conformità all'AI Act.
- Obblighi di accesso a log e metriche.
- Audit e test congiunti.
- Obbligo di notificare vulnerabilità.
- SLA di sicurezza e continuità operativa.

Procedure interne e linee guida

- Procedure per supervisione umana (human oversight).
- Policy interne per uso responsabile dei sistemi AI.
- Linee guida su disclosure, trasparenza e gestione dei contenuti generati.
- Piani di formazione dei dipendenti sull'uso dei sistemi AI e sui rischi associati.

Registrazione e gestione degli incidenti AI

- Moduli o schede per la segnalazione di malfunzionamenti, bias o anomalie.
- Procedure di gestione e risoluzione degli incidenti.
- Log delle azioni correttive e dei follow-up.

Audit e report periodici

- Documentazione dei controlli periodici dei sistemi High-Risk e Limited-Risk.
- Report dei test, dei risultati di monitoraggio e delle eventuali azioni correttive.
- Registro dei miglioramenti implementati in seguito a audit interni o esterni.

Suggerimento pratico

Tutta la documentazione dovrebbe essere centralizzata e facilmente accessibile, idealmente in formato digitale, con versioning chiaro, per permettere aggiornamenti rapidi e audit efficienti.

ROADMAP DI ADEGUAMENTO (2024–2026)

Periodo	Obbligo
2024	Entrata in vigore, divieti immediati
2025	Obblighi per modelli generici (GPAI)
2026	Compliance completa High-Risk

CONCLUSIONE: RIEPILOGO OPERATIVO SULL'AI ACT

Questa dispensa ha l'obiettivo di fornire **tutti gli strumenti pratici per comprendere, valutare e implementare la compliance all'AI Act**. Di seguito, un riepilogo dei punti principali e della strada da intraprendere.

Obiettivi dell'AI Act

- Protezione dei **diritti fondamentali** dei cittadini europei.
- Gestione dei **rischi legati ai sistemi AI** in azienda.
- Promozione di **innovazione sicura e responsabile**.
- Definizione di **classi di rischio e obblighi proporzionati**: Inaccettabile, High-Risk, Limited-Risk, Minimal-Risk.

Classificazione dei rischi

- **Inaccettabile**: vietati già oggi (es. social scoring pubblico, sorveglianza subliminale).
- **High-Risk**: obblighi completi (AIA, registri, supervisione umana, audit, contratti, sicurezza).
- **Limited-Risk**: obblighi di trasparenza e disclosure verso utenti.
- **Minimal-Risk**: nessun obbligo specifico, applicazione di buone pratiche.

Obblighi principali per i sistemi AI

- Creazione di **registro interno AI.**
- Documentazione tecnica e log operativi.
- Valutazioni di impatto (AIA) per High-Risk.
- Supervisione umana e procedure operative.
- Contratti conformi con fornitori (clausole di compliance, audit, SLA, gestione vulnerabilità).
- Trasparenza e formazione dei dipendenti (AI Literacy).
- Meccanismi di gestione degli incidenti.

Guide operative e checklist

- **Checklist interna**: mappatura dei sistemi, classificazione, ruolo degli AI Officer, procedure di human oversight, registro AI, formazione, gestione incidenti.
- **Checklist contratti fornitori**: clausola di conformità, accesso a log e metriche, audit e test congiunti, notifiche vulnerabilità, SLA sicurezza.
- **Altre checklist consigliate**: nuovi sistemi AI, monitoraggio periodico, gestione incidenti, modelli generativi, documentazione e audit esterni.

Documentazione da implementare

- Registro dei sistemi AI.
- Documentazione tecnica dei modelli.
- AI Impact Assessment (AIA) per High-Risk.
- Contratti e accordi con fornitori.
- Procedure interne e linee guida operative.
- Registrazione e gestione incidenti.
- Audit e report periodici.

Roadmap di adeguamento

- **Preparazione e governance**: costituire team AI compliance, definire obiettivi e policy interne.
- **Inventario e classificazione dei sistemi AI**: mappatura dei sistemi, categorizzazione dei rischi, richiesta documentazione ai fornitori.
- **Valutazioni e obblighi di compliance**: AIA, human oversight, aggiornamento registro e contratti.
- **Implementazione operativa**: procedure interne, formazione, integrazione nei processi aziendali.
- **Monitoraggio e miglioramento continuo**: audit, aggiornamento log e metriche, revisione policy e formazione.
- **Prossime scadenze normative**: 2 agosto 2026 per High-Risk (Allegato III)

Conclusione

Seguendo questa dispensa, l'azienda può:

- Comprendere chiaramente **quali sistemi AI sono soggetti a vincoli** e quali rischi comportano.
- **Pianificare un percorso di adeguamento strutturato** e tracciabile.
- Integrare **governance, formazione, contratti e procedure operative** per garantire compliance e ridurre rischi.
- Prepararsi a future **ispezioni o audit** e mantenere un approccio proattivo nell'uso dell'AI.

In sintesi, questa dispensa non è solo un **manuale di compliance**, ma una **guida pratica e operativa** per implementare un'AI **responsabile, sicura e conforme alla normativa europea**, con lo scopo di lasciarvi consapevoli della strada da percorrere.

AVVERA | SB Società Benefit

Sede legale e operativa
20146 Milano
via Sardegna, 21

Sede operativa certificata
21040 Origgio (VA
Largo Umberto Boccioni, 1

Altre sedi
61211 Pesaro (PU)
via Giasone del Maino, 13
33100 Udine (UD)
via G. Tullio, 22

Telefono
+39 0296515401

Fax
0296515499

C.F./P.IVA 06047090961
Cap. Soc. 300.000 euro I.V.
Reg. Impo. MI
06047090961
REA 1866500

www.avvera.it
avvera@legalmail.it

IMQ CERTIFIED QUALITY MANAGEMENT SYSTEM ISO 9001:2015
IMQ CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEM ISO/IEC 27001:2022
IMQ CERTIFIED OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM ISO 45001:2018