

AI ACT

AI Act: guida pratica per le Aziende

Le regole che aiutano l'azienda a proteggersi nell'uso dell'intelligenza artificiale

White Paper pratico per imprenditori, manager e key user delle PMI

Il quadro normativo: perché esiste l'AI Act

L'intelligenza artificiale è già entrata nelle aziende attraverso assistenti digitali, chatbot, funzioni intelligenti integrate nei software e piattaforme come Microsoft Copilot. Per accompagnare questa trasformazione, l'Unione Europea ha introdotto il Regolamento (UE) 2024/1689, conosciuto come AI Act: un quadro normativo organico per favorire un uso affidabile, trasparente e controllato dell'AI.

Il principio alla base della norma è semplice

Più un sistema AI può incidere su persone, diritti, sicurezza o decisioni importanti, maggiore deve essere il livello di controllo richiesto. Per una Azienda questo non significa creare burocrazia, ma introdurre consapevolezza, responsabilità e tracciabilità negli strumenti che le persone utilizzano ogni giorno.

PERCHÉ RIGUARDA TUTTE LE AZIENDE, ANCHE LE PMI

L'AI Act non interessa solo chi sviluppa tecnologia. Riguarda anche le aziende che usano strumenti AI di terzi, comprese quelle che adottano Copilot, chatbot aziendali o servizi di AI generativa. Tutte le Aziende, anche le PMI devono quindi sapere quali strumenti vengono usati, formare le persone, adottare regole interne, applicare trasparenza quando richiesta e mantenere controllo umano sugli output.

Dalla compliance all'autotutela aziendale

Le misure richieste coincidono con ciò che un'azienda prudente dovrebbe fare comunque: proteggere dati e know-how, chiarire responsabilità, evitare decisioni non controllate e ridurre il rischio di output errati.

Dati fuori controllo

Offerte, listini, contratti o informazioni cliente possono finire in servizi non approvati.

Output non verificati

Una risposta può sembrare corretta ma contenere errori. La responsabilità resta aziendale.

Adozione invisibile

La Shadow AI rende difficile dimostrare cosa viene usato, da chi e per quali scopi.

Cosa significa davvero AI Act per una Azienda

Il tema centrale non è solo “essere conformi”, ma governare una tecnologia che molte persone stanno già usando nei processi quotidiani.

L’AI Act distingue gli usi dell’intelligenza artificiale in base al rischio. Alcuni impieghi sono vietati, altri richiedono controlli rafforzati, altri ancora comportano obblighi di trasparenza. Nelle PMI, tuttavia, il rischio più frequente è spesso più semplice e più vicino all’operatività: l’uso non coordinato di strumenti AI per scrivere testi, analizzare documenti, generare contenuti o preparare risposte ai clienti.

Livello	Esempi per l’azienda	Implicazione concreta
VIETATO	Pratiche manipolative, social scoring e altri usi proibiti	Bloccare il caso d’uso e attivare escalation direzionale o legale.
ALTO RISCHIO	HR, accesso a servizi, credito, sicurezza, prodotti regolati o decisioni critiche	Richiede assessment rafforzato, documentazione, supervisione e validazione specialistica.
TRASPARENZA	Chatbot, assistenti virtuali, contenuti generati o manipolati con AI	Informare l’utente e conservare evidenza delle modalità adottate.
BASSO / MINIMO	Supporto a scrittura, riassunti, bozze, produttività personale	Policy d’uso, formazione, protezione dei dati e controllo umano.

Shadow AI: il rischio più diffuso

La Shadow AI nasce quando le persone usano strumenti non approvati o non visibili all’azienda. Può accadere per velocizzare attività quotidiane: preparare un’offerta, sintetizzare un contratto, produrre una bozza marketing, tradurre contenuti o rispondere a un cliente. Il problema non è l’intenzione, ma l’assenza di controllo su dati, qualità dell’output e responsabilità.

EXECUTIVE GUIDE

L’AI Act aiuta l’impresa a trasformare un uso spontaneo e disordinato dell’AI in un modello governato. Il punto non è vietare gli strumenti, ma renderli visibili, autorizzati, comprensibili e controllati.

Offerte e contratti

Evitare di caricare testi riservati su servizi non autorizzati.

Marketing e contenuti

Verificare fonti, claim, copyright e trasparenza quando necessario.

HR e persone

Trattare ogni uso su candidati o dipendenti come caso sensibile da valutare.

Gli obblighi minimi da rendere operativi

Questa è la parte più importante: gli obblighi minimi coincidono con le misure che proteggono l'azienda da errori, fughe di dati e decisioni non controllate.

Per una Azienda l'obiettivo non è costruire un sistema complesso, ma introdurre pochi presidi reali, comprensibili e verificabili. Registro AI, formazione, policy, trasparenza, classificazione e controllo umano devono funzionare insieme: solo così la conformità diventa una forma concreta di autotutela.

Obbligo minimo	Valore executive	Spiegazione operativa
Registro AI	Sapere cosa viene usato	È l'inventario degli strumenti AI, dei dati trattati, degli utenti, delle finalità e dei responsabili. Non è burocrazia: è la mappa che consente alla Direzione di capire dove l'AI è già presente e dove servono controlli.
AI Literacy	Formare e documentare	Le persone devono conoscere limiti, rischi, uso dei dati e responsabilità. La formazione va tracciata con presenze, materiali o attestati, perché l'azienda deve poter dimostrare di aver abilitato un uso consapevole.
Policy AI	Regole semplici e condivise	La policy chiarisce strumenti autorizzati, dati vietati, verifica degli output e comportamenti non consentiti. Senza una policy ogni reparto crea regole proprie, aumentando il rischio di incoerenze.
Trasparenza	Fiducia verso utenti e clienti	Quando un utente interagisce con un sistema AI deve capirlo chiaramente. La trasparenza non è solo un obbligo: evita equivoci e rafforza la credibilità dell'azienda.
Classificazione	Capire quando il rischio cresce	Ogni nuovo strumento o nuovo uso deve essere valutato prima del rilascio. I casi che toccano HR, scoring, sicurezza, prodotti regolati o decisioni critiche richiedono attenzione rafforzata.
Controllo umano	La responsabilità resta all'azienda	L'AI può suggerire, sintetizzare e produrre bozze, ma documenti destinati a clienti e decisioni rilevanti devono essere verificati da persone competenti. Il controllo umano riduce errori e responsabilità.

VADEMECUM OPERATIVO

La prima applicazione può essere leggera: un Registro AI in formato tabellare, una policy di una pagina, un piano di formazione tracciato, una procedura di approvazione per nuovi strumenti e un canale per segnalare errori o usi impropri.

La policy in cinque regole

- 1 Usare solo strumenti approvati o censiti nel Registro AI.
- 2 Non caricare dati cliente, credenziali, contratti o informazioni riservate in servizi non autorizzati.
- 3 Verificare ogni output destinato a clienti, pubblicazioni o decisioni rilevanti.
- 4 Informare l'utente quando interagisce direttamente con un sistema AI.
- 5 Segnalare anomalie, errori gravi, output discriminatori o possibili esposizioni di dati.

Roadmap operativa per i primi 90 giorni

Il percorso deve essere progressivo: prima si rende visibile l'uso dell'AI, poi si introducono regole, formazione e controlli.

Periodo	Focus	Risultato atteso
0-30 giorni	Fotografia iniziale	Censire strumenti ufficiali e informali, account personali, casi d'uso, reparti coinvolti e categorie di dati trattati. L'obiettivo è rendere visibile ciò che oggi può essere disperso.
30-60 giorni	Governance e regole	Definire sponsor di Direzione, referente operativo, policy AI, elenco strumenti autorizzati, Registro AI e processo di approvazione dei nuovi strumenti.
60-90 giorni	Formazione e controllo	Erogare AI Literacy per ruoli, classificare i casi sensibili, introdurre verifica degli output, canale incidenti e calendario di revisione periodica.

Checklist per la Direzione

☐	Sappiamo quali strumenti AI sono usati oggi, anche in modo informale?
☐	Esiste un elenco chiaro di strumenti approvati, tollerati e vietati?
☐	Le persone sanno quali dati non devono mai caricare in strumenti non autorizzati?
☐	Gli output importanti sono verificati da una persona competente prima dell'uso?
☐	La formazione AI Literacy è documentata e aggiornata?
☐	Chatbot e assistenti dichiarano chiaramente l'interazione con AI quando richiesto?
☐	I casi HR, scoring, sicurezza o prodotti regolati sono stati separati e valutati?

Il ruolo di Sogesi

Come Microsoft Partner orientato all'adozione dell'AI, Sogesi supporta le Aziende nella mappatura degli strumenti, classificazione dei casi d'uso, costruzione di registro e policy, formazione AI Literacy, trasparenza e riduzione della Shadow AI. Il risultato è un modello sostenibile, pragmatico e coerente con l'utilizzo di soluzioni Microsoft.

MESSAGGIO FINALE

L'AI Act non è un freno all'innovazione

È una guida per usare l'intelligenza artificiale in modo più sicuro, produttivo e responsabile. Le aziende che introducono regole semplici e strumenti approvati proteggono meglio il proprio patrimonio informativo e creano le condizioni per adottare l'AI con fiducia.

Nota e fonti utilizzate

Documento informativo e organizzativo. Non sostituisce parere legale specialistico. Contenuti elaborati esclusivamente dai documenti ufficiali pubblicati dalla Commissione Europea alla data del 6 luglio 2026.