

COME APPLICARE L'AI ACT

Esempi pratici di impiego dell'IA nelle aree aziendali

White paper operativo per una adozione dell'IA governata, proporzionata e documentata

Il documento analizza casi d'uso frequenti di Microsoft Copilot nelle principali aree aziendali, ne individua il grado di rischio ai sensi dell'AI Act, indica le misure organizzative da adottare e segnala le condizioni che imporrebbero una nuova valutazione.

Percorso di lettura	Cosa consente di governare
01 Area Commerciale	Revisione umana delle offerte, verifica dei dati economici e perimetro dei documenti utilizzabili
02 Area Marketing	Trasparenza dei contenuti, responsabilità editoriale e divieto di contenuti ingannevoli
03 Area Amministrazione	Anomalie trattate come segnalazioni da verificare, senza decisioni automatiche
04 Area HR	Materiali informativi governati e confine con selezione e valutazione dei lavoratori
05 Area Acquisti	Criteri di confronto definiti, riservatezza delle offerte e decisione finale umana
06 Area Customer Care	Supervisione sostanziale delle risposte tecniche e citazione verificabile delle fonti
Obblighi comuni	Registro dei casi d'uso, AI literacy, supervisione, dati, permessi Microsoft 365 e rivalutazione
Conclusione operativa	Quattro presidi da introdurre subito e ambiti che richiedono un controllo più rigoroso

01 | Valutazione di singoli casi d'uso frequenti

1. Area Commerciale

Caso analizzato

Preparazione di una proposta commerciale utilizzando offerte precedenti, email del cliente, note di riunione e documentazione tecnica, con produzione di:

■ bozza di offerta;	■ sintesi delle esigenze;	■ elenco dei punti aperti;
■ scaletta della presentazione commerciale.		

Grado di rischio

Rischio minimo o limitato.

Copilot svolge una funzione di assistenza alla redazione e all'analisi documentale. Non decide se il cliente abbia diritto a un servizio, non effettua un credit scoring su persone fisiche e non assume una decisione contrattuale in autonomia.

Cosa dovrebbe fare l'azienda

1. **Prevedere una revisione umana obbligatoria** prima dell'invio dell'offerta.
2. **Verificare dati economici, requisiti, prezzi, scadenze e impegni contrattuali**, perché Copilot può produrre informazioni inesatte o non aggiornate.
3. **Definire quali documenti possono essere utilizzati**, evitando che offerte riservate di altri clienti o informazioni non pertinenti vengano richiamate nel nuovo documento.
4. **Controllare le autorizzazioni di Microsoft 365**, applicando il principio per cui l'utente deve poter utilizzare con Copilot solo le informazioni alle quali è già legittimamente autorizzato.
5. **Evitare l'inserimento di categorie particolari di dati personali** non necessarie alla proposta.
6. **Conservare la responsabilità commerciale in capo a una persona identificata**, per esempio il responsabile della proposta o l'account manager.
7. **Formare gli utilizzatori**, spiegando limiti, rischi di allucinazione, protezione dei dati e modalità di verifica degli output.

L'articolo 4 richiede che il personale che utilizza sistemi di IA disponga di un livello adeguato di alfabetizzazione in materia di IA, tenendo conto delle competenze, dell'esperienza e del contesto d'uso.

<https://artificialintelligenceact.eu/article/4/>

<https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>

Quando potrebbe aumentare il rischio

Il caso deve essere rivalutato se Copilot viene utilizzato per:

■ attribuire automaticamente un rating al cliente;	■ determinare prezzi o condizioni sulla base di caratteristiche personali;	■ valutare l'affidabilità creditizia di persone fisiche;
■ accettare o rifiutare automaticamente una richiesta;	■ inviare autonomamente offerte senza approvazione umana.	

2. Area Marketing

Caso analizzato

Creazione di newsletter, articoli per il blog, post LinkedIn, DEM, presentazioni, oggetti email e contenuti per landing page, a partire da materiali aziendali già validati

Grado di rischio

Rischio minimo, con attenzione agli **obblighi di trasparenza** relativi ai contenuti generati o manipolati dall'IA.

La produzione di normali contenuti commerciali, promozionali o informativi non rientra di per sé tra i sistemi ad alto rischio. Il livello cambia se il contenuto viene utilizzato in modo manipolativo, impersona persone reali, costituisce un deepfake oppure viene presentato come informazione autentica su questioni di interesse pubblico senza adeguata supervisione editoriale.

Cosa dovrebbe fare l'azienda

1. **Sottoporre ogni contenuto a revisione editoriale umana** prima della pubblicazione.
2. **Verificare affermazioni, dati, statistiche, citazioni, testimonianze e riferimenti normativi.**
3. **Accertare la titolarità o la licenza dei materiali utilizzati**, come fotografie, testi, marchi, casi cliente e documenti di terzi.
4. **Non pubblicare informazioni riservate**, dati personali o riferimenti a clienti senza una valida base giuridica o autorizzazione.
5. **Definire una regola aziendale sulla trasparenza**, specificando quando dichiarare che un contenuto è stato generato o assistito dall'IA.
6. **Identificare il responsabile editoriale** che approva il contenuto e ne assume la responsabilità.
7. **Vietare espressamente contenuti ingannevoli**, recensioni artificiali, testimonianze inventate, immagini capaci di indurre il pubblico a credere che un evento mai avvenuto sia reale.
8. **Documentare il processo di approvazione**, almeno per campagne, articoli istituzionali e contenuti potenzialmente sensibili.

L'AI Act disciplina specificamente la trasparenza di determinati sistemi e contenuti sintetici nell'articolo 50. Non tutti i testi assistiti dall'IA richiedono automaticamente un'etichetta pubblica, ma la valutazione deve considerare il tipo di contenuto, il pubblico, il possibile carattere ingannevole e la presenza di un'effettiva responsabilità editoriale.

<https://artificialintelligenceact.eu/article/50/>

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1689>

Quando potrebbe aumentare il rischio

Il caso diventa sensibilmente più delicato se vengono prodotti:

■ deepfake audio o video;	■ finte dichiarazioni attribuite a persone reali;	■ contenuti che imitano una fonte giornalistica;
■ campagne personalizzate utilizzando dati sensibili;	■ messaggi progettati per sfruttare vulnerabilità dovute a età, disabilità o condizioni socioeconomiche;	■ contenuti politici o relativi a temi di rilevante interesse pubblico.

3. Area Amministrazione

Caso analizzato

Analisi di file Excel o report amministrativi per rilevare scostamenti, anomalie, trend, fatture in ritardo o variazioni significative nei comportamenti dei clienti.

Grado di rischio

Rischio minimo o limitato, a condizione che l'output resti un supporto all'analisi.

L'individuazione di anomalie in dati amministrativi o finanziari aziendali non è automaticamente un'attività ad alto rischio. Il risultato suggerisce elementi da verificare, ma non dovrebbe produrre autonomamente conseguenze giuridiche o economiche nei confronti di una persona.

Cosa dovrebbe fare l'azienda

1. **Trattare anomalie e scostamenti come segnalazioni da verificare**, non come fatti accertati.
2. **Far validare i risultati da amministrazione, controllo di gestione o direzione finanziaria.**
3. **Definire chiaramente le fonti dati**, il periodo analizzato e il significato degli indicatori.
4. **Controllare completezza, aggiornamento e qualità dei dati** prima di richiedere l'elaborazione.
5. **Evitare decisioni automatiche**, come bloccare un cliente, sospendere una fornitura o modificare condizioni di pagamento sulla sola base dell'output.
6. **Proteggere dati bancari, contabili e personali**, applicando autorizzazioni, criteri di conservazione e minimizzazione.
7. **Documentare le verifiche effettuate** quando l'analisi contribuisce a una decisione economicamente significativa.
8. **Affiancare l'AI Act al GDPR**, quando i dati analizzati sono riferibili a persone fisiche, ditte individuali, professionisti o garanti.

Quando potrebbe diventare ad alto rischio

È necessaria una nuova classificazione se il sistema viene utilizzato per:

■ valutare l'affidabilità creditizia di persone fisiche;	■ stabilire automaticamente l'accesso a un servizio essenziale;	■ prendere decisioni esclusivamente automatizzate con effetti giuridici rilevanti;
--	---	--

■ profilare sistematicamente clienti persone fisiche;	■ determinare automaticamente condizioni economiche individuali.	
---	--	--

L'Allegato III include tra i casi ad alto rischio determinati impieghi relativi all'affidabilità creditizia delle persone fisiche e all'accesso a servizi privati essenziali.

<https://artificialintelligenceact.eu/annex/3/>

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1689>

4. Area HR

Caso analizzato

Preparazione di materiali di onboarding, FAQ interne, procedure operative, piani formativi, kit di benvenuto e comunicazioni al personale.

Grado di rischio

Rischio minimo o limitato.

La classificazione dipende dalla finalità, non dalla denominazione "HR". La semplice produzione di documenti informativi per i dipendenti non è un utilizzo ad alto rischio.

Cosa dovrebbe fare l'azienda

1. **Utilizzare esclusivamente documenti HR approvati e aggiornati** come fonti.
2. **Far approvare i materiali dall'ufficio HR o dal responsabile competente.**
3. **Evitare di utilizzare Copilot come fonte definitiva** per informazioni su contratti, retribuzioni, ferie, procedimenti disciplinari, sicurezza o diritti dei lavoratori.
4. **Non inserire dati sanitari, disciplinari, sindacali o altre informazioni particolarmente sensibili** se non strettamente necessario e giuridicamente autorizzato.
5. **Comunicare ai dipendenti che il contenuto è informativo**, indicando il referente umano al quale rivolgersi per chiarimenti.
6. **Verificare accessibilità, assenza di discriminazioni e coerenza linguistica** dei materiali generati.
7. **Mantenere versionamento, data di approvazione e titolarità del documento.**
8. **Formare il personale HR a riconoscere errori, distorsioni e possibili bias.**

Confine da non superare senza nuova valutazione

L'impiego diventerebbe potenzialmente **ad alto rischio** se Copilot o un sistema collegato venisse utilizzato per:

■ selezionare o filtrare curriculum;	■ attribuire punteggi ai candidati;	■ decidere assunzioni o promozioni;
■ valutare le prestazioni;	■ assegnare compiti sulla base di caratteristiche personali;	■ monitorare comportamento o produttività;

■ suggerire licenziamenti o provvedimenti disciplinari.		
---	--	--

I sistemi destinati al reclutamento, alla selezione, alla gestione dei lavoratori, alla valutazione delle prestazioni o a decisioni che incidono sul rapporto di lavoro sono espressamente contemplati nell'area "occupazione e gestione dei lavoratori" dell'Allegato III.

<https://artificialintelligenceact.eu/annex/3/>

<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1689>

In una simile configurazione diventerebbero rilevanti gli obblighi rafforzati per i deployer: uso conforme alle istruzioni, supervisione umana affidata a persone competenti e dotate di autorità, controllo dei dati di input, monitoraggio, conservazione dei log e gestione degli incidenti.

<https://artificialintelligenceact.eu/article/26/>

5. Area Acquisti

Caso analizzato

Sintesi delle offerte dei fornitori, confronto dei preventivi, preparazione di matrici comparative, individuazione delle differenze tecniche ed economiche e predisposizione di richieste da inviare ai fornitori.

Grado di rischio

Rischio minimo o limitato.

Il confronto tra offerte commerciali di imprese non rientra tra gli impieghi ad alto rischio elencati dall'AI Act. Copilot svolge una funzione istruttoria e la decisione di acquisto rimane all'azienda.

Cosa deve fare l'azienda

1. **Definire preventivamente i criteri di confronto**, evitando che sia Copilot a inventare pesi o criteri non approvati.
2. **Verificare manualmente prezzi, quantità, imposte, scadenze, condizioni di pagamento e livelli di servizio.**
3. **Mantenere la decisione finale in capo al responsabile acquisti o all'organo autorizzato.**
4. **Proteggere la riservatezza delle offerte**, evitando la divulgazione dei prezzi di un fornitore ad altri concorrenti.
5. **Accertare che i documenti appartengano alla stessa procedura di acquisto e siano aggiornati.**
6. **Documentare motivazione e approvazione della scelta**, soprattutto per acquisti rilevanti.
7. **Verificare eventuali distorsioni**, per esempio confronti incompleti dovuti a formati diversi o clausole non rilevate.
8. **Non lasciare che il sistema escluda automaticamente un fornitore** senza una verifica umana.

Quando potrebbe aumentare il rischio

Il rischio cambierebbe se il confronto fosse utilizzato per:

■ valutare persone fisiche anziché imprese;	■ inferire caratteristiche personali protette;	■ generare blacklist automatiche;
■ adottare decisioni completamente automatizzate con effetti significativi;	■ utilizzare dati ottenuti in modo illegittimo o non pertinente.	

6. Area Customer Care

Caso analizzato

L'area Customer Care dispone di:

■ manuali tecnici dei prodotti;	■ una libreria di soluzioni applicabili ai problemi tecnici;	■ un agente di IA che consulta queste fonti per elaborare la risposta al quesito del cliente;
■ un sistema di citazione delle fonti utilizzate;	■ un processo nel quale la risposta viene inoltrata prima a un Responsabile;	■ un controllo umano preventivo, dopo il quale il Responsabile può approvare, modificare o respingere la risposta;
■ l'invio al cliente effettuato esclusivamente dal Responsabile.		

L'agente, quindi, non comunica autonomamente con il cliente e non chiude autonomamente la richiesta. Produce una **proposta di risposta tecnica documentata**, sottoposta a verifica umana prima dell'utilizzo.

Grado di rischio

Rischio minimo o limitato, con un livello di attenzione operativa superiore rispetto a un semplice impiego redazionale.

Nella configurazione descritta, l'agente svolge una funzione di ricerca documentale, sintesi e supporto alla risposta. Non assume decisioni autonome nei confronti del cliente, non determina l'accesso a un servizio essenziale e non rientra, per la sola attività di assistenza tecnica, negli ambiti ad alto rischio elencati dall'Allegato III dell'AI Act. La presenza di una revisione umana effettiva prima dell'invio rafforza questa valutazione.

<https://artificialintelligenceact.eu/annex/3/>

<https://artificialintelligenceact.eu/article/6/>

La classificazione come rischio minimo o limitato non significa, tuttavia, che l'utilizzo sia privo di conseguenze. Una risposta tecnica errata potrebbe provocare:

■ un malfunzionamento;	■ un'interruzione del servizio;	■ una configurazione non corretta;
■ perdita o alterazione di dati;	■ esposizione a vulnerabilità informatiche;	■ decadenza di garanzie;
■ conseguenze sulla sicurezza, qualora il prodotto abbia funzioni critiche.		

Per questo motivo la supervisione umana deve essere **sostanziale** e non limitarsi a un'approvazione formale.

Sintesi della valutazione

Elemento del caso	Valutazione
Ricerca nei manuali e nella knowledge base	Attività di supporto a rischio minimo
Generazione della risposta tecnica	Rischio limitato, da controllare per accuratezza e completezza
Citazione delle fonti	Misura positiva di tracciabilità, ma non prova automatica della correttezza
Invio preliminare al Responsabile	Misura centrale di supervisione umana
Invio al cliente solo dopo approvazione	Evita l'interazione autonoma dell'agente con il cliente
Esecuzione automatica di azioni sul prodotto	Non prevista; richiederebbe una nuova valutazione

Per approfondire: si raccomanda la consultazione del documento dedicato **AI NEL CUSTOMER CARE** che descrive in modo operativo gli strumenti idonei a supportare la supervisione umana — quali workflow di approvazione, registri delle verifiche, tracciamento delle fonti e controlli di escalation — ed i criteri con cui valutare la qualità delle risposte generate.

02 | Obblighi comuni da applicare a tutti i casi

Anche quando il rischio è minimo, “rischio minimo” **non significa assenza di regole**. Per i casi esaminati sono suggerite le seguenti misure.

1. Registro dei casi d'uso

Per ogni utilizzo registrare:

▪ area aziendale;	▪ finalità;	▪ utenti autorizzati;
▪ tipologia di dati utilizzati;	▪ output prodotto;	▪ soggetti interessati;
▪ responsabile del controllo umano;	▪ livello di rischio;	▪ data dell'ultima valutazione.

2. AI Literacy

L'azienda deve assicurare un livello adeguato di competenza a chi utilizza Copilot. La formazione deve essere proporzionata al ruolo e al contesto e dovrebbe comprendere almeno:

▪ funzionamento generale dell'IA generativa;	▪ possibilità di errori e allucinazioni;	▪ verifica delle fonti;
▪ protezione dei dati;	▪ gestione delle informazioni riservate;	▪ copyright;
▪ supervisione umana;	▪ escalation in caso di output anomalo.	

L'articolo 4 adotta un approccio contestuale e non prescrive necessariamente uno specifico certificato o un unico formato formativo.

<https://artificialintelligenceact.eu/article/4/>

<https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>

3. Supervisione umana

Ogni output deve essere considerato una **bozza o un supporto**, non una decisione aziendale definitiva. L'azienda deve identificare chi:

▪ verifica il contenuto;	▪ può modificarlo o respingerlo;	▪ ne autorizza l'utilizzo;
▪ assume la responsabilità della decisione finale.		

4. Regole sull'utilizzo dei dati

Occorre stabilire in modo esplicito:

▪ quali dati possono essere inseriti;	▪ quali dati non possono essere utilizzati;	▪ come trattare dati personali e categorie particolari;
▪ quali documenti sono autorizzati come fonti;	▪ come gestire le informazioni dei clienti e dei fornitori;	▪ come applicare il principio di minimizzazione.

5. Controllo delle autorizzazioni Microsoft 365

Prima di ampliare l'utilizzo di Copilot è opportuno verificare:

▪ permessi e condivisioni SharePoint;	▪ accessi a Teams e OneDrive;	▪ siti o cartelle sovraesposti;
▪ documenti obsoleti;	▪ etichette di riservatezza;	▪ politiche di conservazione;
▪ accessi di utenti esterni.		

6. Processo di rivalutazione

La classificazione deve essere ripetuta quando:

▪ cambia la finalità;	▪ si aggiungono nuove fonti dati;	▪ l'output influenza persone fisiche;
▪ viene eliminata o ridotta la revisione umana;	▪ Copilot viene integrato con Power Automate o sistemi gestionali;	▪ il sistema esegue automaticamente azioni;
▪ vengono introdotti punteggi, ranking o profilazioni.		

03 | Conclusione pratica

I casi contenuti nel documento possono essere adottati con un **regime di governance proporzionato e relativamente leggero**, perché si basano sulla produzione di bozze, sintesi e analisi preliminari. La condizione determinante è che:

- **Copilot assista la persona, senza sostituirla nelle decisioni che producono effetti giuridici, economici o professionali significativi.**

L'azienda dovrebbe quindi introdurre subito quattro presidi: **formazione documentata, revisione umana, regole sui dati e registro dei casi d'uso**. Per l'HR e l'amministrazione è inoltre opportuno prevedere un controllo più rigoroso, perché un'evoluzione verso selezione, valutazione dei lavoratori, credit scoring o decisioni automatizzate potrebbe portare il sistema nel perimetro dell'alto rischio.

Avvertenza: questo documento costituisce una valutazione operativa basata sul Regolamento (UE) 2024/1689 e non sostituisce un parere legale. La classificazione deve essere riesaminata se cambiano la finalità, le fonti informative, il livello di automazione o gli effetti dell'output.