



Copilot è sicuro per i dati della tua azienda?

Quali versioni usare, come Microsoft protegge i dati e le zone grigie che fanno la differenza

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Indice

Come usare questa dispensa ... 3

1. Dove finiscono quei dati? ... 3

2. Non esiste un solo Copilot ... 4

2.1 Il trucco dei due secondi: lo scudo verde ... 5

2.2 Microsoft 365 Copilot ... 6

3. Come Microsoft protegge i dati ... 6

3.1 I tuoi dati non vanno a scuola ... 6

3.2 Copilot vede solo quello che vedi tu ... 7

3.3 Etichette di riservatezza e regole di conservazione ... 7

3.4 Contratto, GDPR e Data Boundary ... 7

4. Le zone grigie ... 8

4.1 Le ricerche sul web ... 8

4.2 L'ora di punta: il flex routing ... 9

4.3 I modelli di intelligenza artificiale ... 10

4.4 L'oversharing: il rischio più importante ... 11

4.5 La valutazione d'impatto ... 12

5. La lista di controllo ... 13

Il controllo in venti minuti ... 14

Le domande che arrivano in aula ... 15

Glossario ... 15

Per approfondire ... 16

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Capire quali versioni di Copilot sono adatte ai dati aziendali, che cosa garantisce Microsoft e quali controlli fare prima di usarlo in azienda.

Che cosa saprai fare alla fine

- Riconoscere una versione personale da una versione di lavoro di Copilot.
- Spiegare le quattro protezioni principali delle versioni di lavoro.
- Individuare le eccezioni: ricerche sul web, flex routing e modelli Claude.
- Riconoscere il rischio di oversharing e sapere quando serve una valutazione d'impatto.
- Applicare in azienda una lista di controllo in cinque punti.

1. Dove finiscono quei dati?

Copilot è sicuro per i dati della tua azienda? Sì, ma solo se è la versione giusta, se è configurato bene e se le persone sanno usarlo.

Immagina questa scena. È lunedì mattina e una tua collega deve preparare un'offerta in fretta. Apre Copilot, incolla il listino prezzi, il contratto del cliente, magari anche qualche dato personale. Dieci secondi, e l'offerta è pronta. Comodo. Ma dove sono finiti quei dati?

La risposta è: dipende. Dipende da quale Copilot ha usato e da come è configurato. Questa dispensa segue il video in tre tappe: quali versioni vanno bene per i dati aziendali, come Microsoft li protegge e quali sono le zone grigie, cioè i dettagli che fanno la differenza tra un uso tranquillo e un brutto pasticcio.

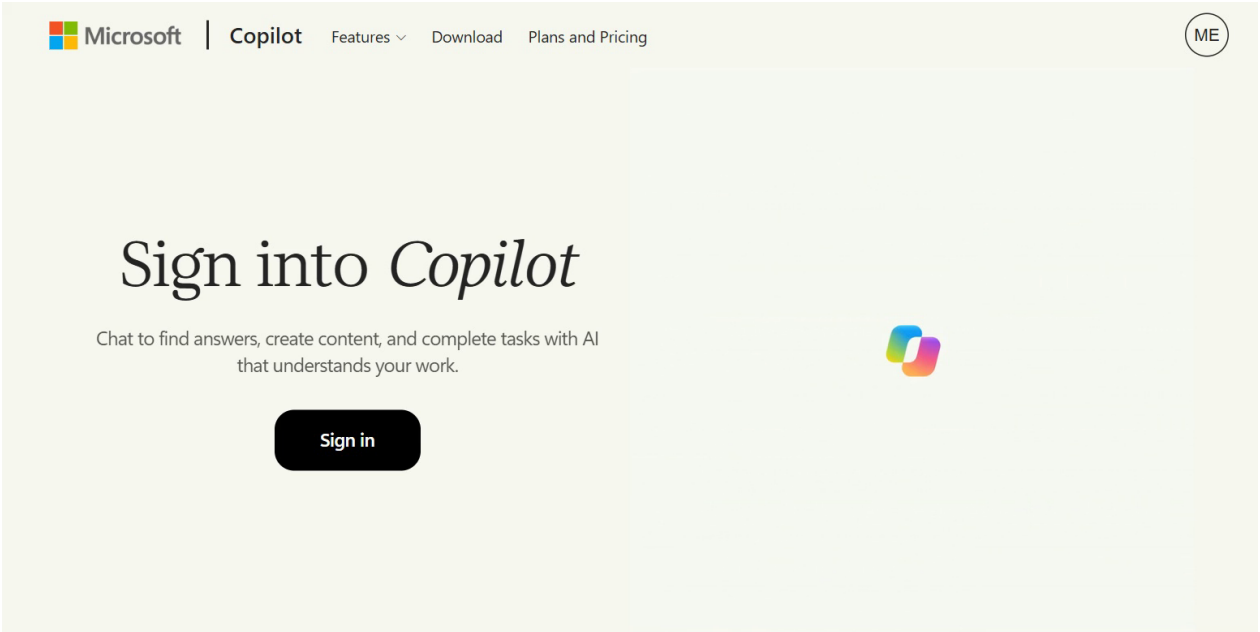
> **L'IDEA IN UNA RIGA**
>
> Copilot non crea i rischi dal nulla: eredita le regole, e i disordini, che trova in azienda.

2. Non esiste un solo Copilot

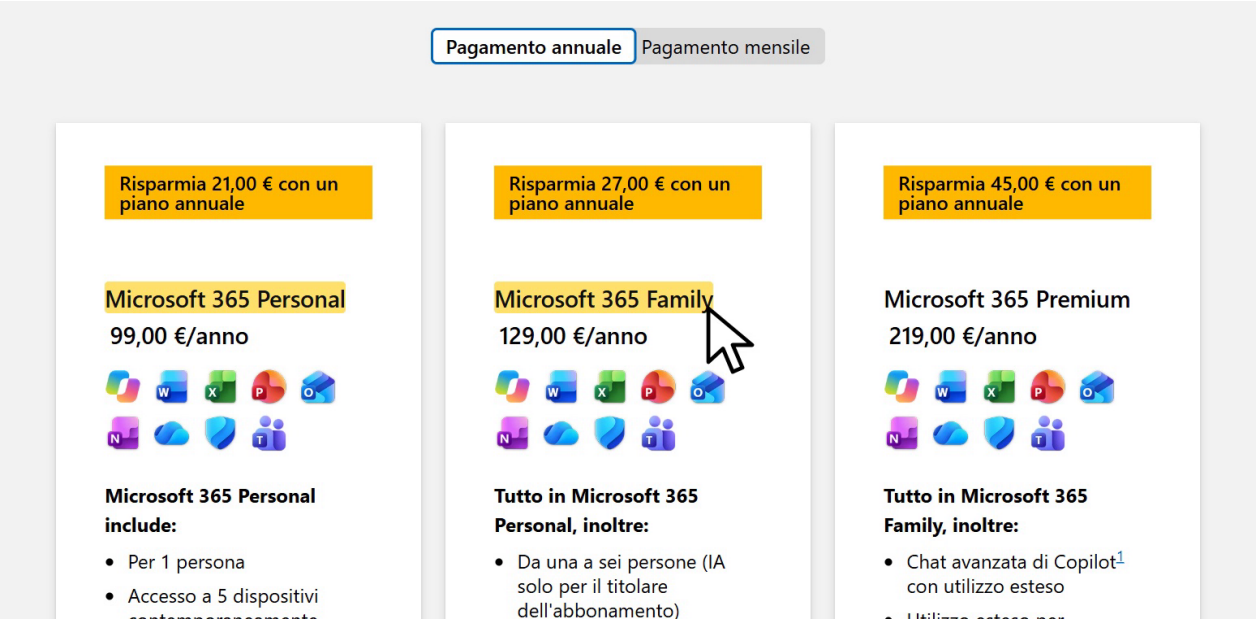
«Copilot» è un nome solo, ma dietro ci sono prodotti diversi. Un po' come la parola «auto»: l'utilitaria con cui vai a fare la spesa e il furgone aziendale con l'assicurazione per le merci si chiamano allo stesso modo, ma non sono fatti per lo stesso lavoro.

Versione	Come ci entri	Dati dell'azienda
Copilot gratuito (Windows, browser)	Account personale Microsoft	No: mancano le garanzie contrattuali per le aziende
Copilot in Microsoft 365 Personal e Family	Account personale con abbonamento	No: è pensato per privati e famiglie
Copilot Chat con account di lavoro	Account aziendale Microsoft 365	Sì, con protezione dei dati aziendali. Senza licenza aggiuntiva lavora sui dati web
Microsoft 365 Copilot (a pagamento)	Account aziendale con licenza	Sì, e può leggere documenti ed email a cui hai accesso: va configurato con attenzione

Le versioni di Copilot in base all'uso. I dettagli delle licenze cambiano spesso: fa fede la pagina Microsoft.



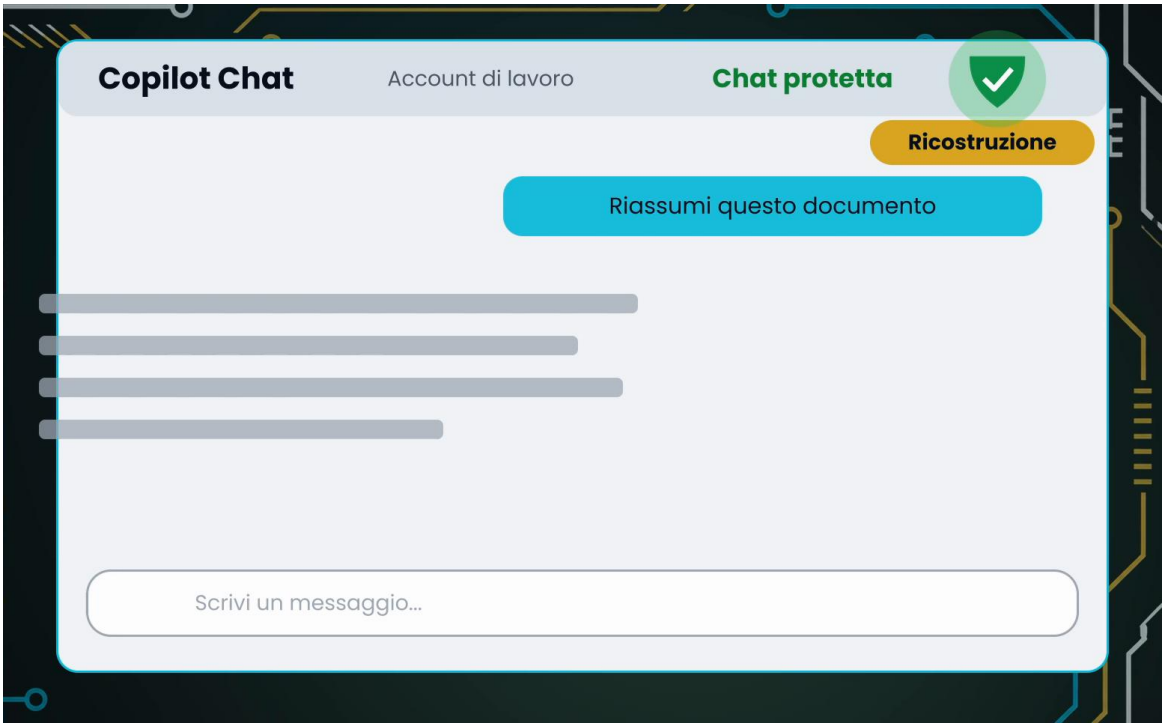
La pagina di accesso di Copilot: il prodotto è uno solo di nome, ma l'account con cui entri cambia le garanzie.



Microsoft 365 Personal e Family: abbonamenti per privati e famiglie, anche se includono Copilot.

2.1 Il trucco dei due secondi: lo scudo verde

Quando usi Copilot Chat con l'account di lavoro, compare uno **scudo verde**: è il segnale che la chat è protetta. Se lo scudo c'è, sei nella versione aziendale. Se non c'è, fermati: probabilmente stai usando una versione personale, quindi controlla con quale account sei entrato.



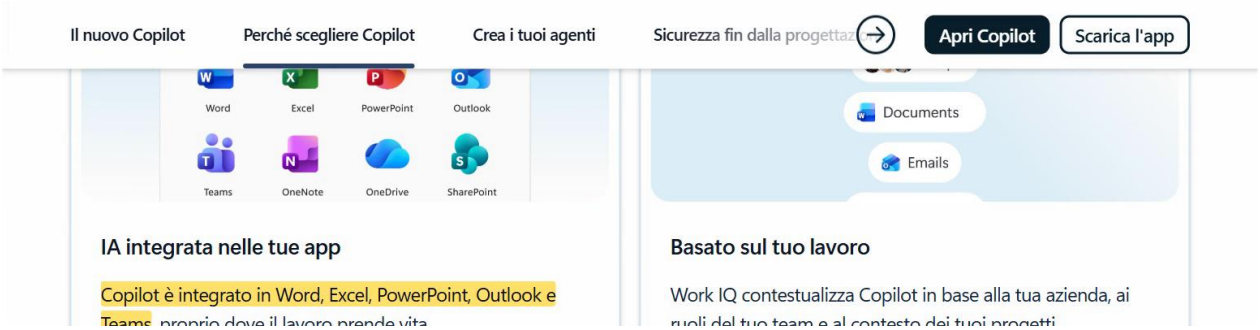
Ricostruzione a scopo didattico, non è una schermata di Microsoft: lo scudo verde indica la protezione dei dati aziendali. Il suo aspetto può cambiare nel tempo.

UN SEGNALE, NON UNA GARANZIA

L'aspetto e la posizione dello scudo possono cambiare con gli aggiornamenti. In caso di dubbio guarda l'account in uso e chiedi a chi gestisce l'informatica dell'azienda.

2.2 Microsoft 365 Copilot

È la versione a pagamento per le aziende. Lavora direttamente dentro Word, Excel, Outlook e Teams e può leggere i documenti e le email dell'azienda a cui hai accesso. Proprio per questo va configurata con attenzione.



La pagina di Copilot per le aziende: integrato in Word, Excel, PowerPoint, Outlook e Teams.

UNA NOTA SUL NOME

Microsoft sta rinominando i prodotti: nelle pagine più recenti Microsoft 365 Copilot compare come «Microsoft Copilot» e Microsoft 365 Copilot Chat come «Microsoft Copilot Chat». Se trovi nomi diversi da quelli di questa dispensa, controlla la tabella delle licenze sulla documentazione ufficiale.

3. Come Microsoft protegge i dati

Nelle versioni di lavoro Microsoft garantisce quattro cose. Sono impegni scritti nella documentazione e nel contratto: vale la pena leggerli direttamente.

3.1 I tuoi dati non vanno a scuola

Quello che scrivi, i documenti che Copilot legge tramite Microsoft Graph e le risposte che ti dà non vengono usati per addestrare i modelli di base, cioè i programmi che generano le risposte. Il contratto del tuo cliente non diventa materiale di studio per l'intelligenza artificiale.

- **I dati non vengono usati per eseguire il training dei modelli di base**: Microsoft Copilot Chat usa il contesto dell'utente per creare risposte pertinenti. Microsoft Copilot usa anche i dati di Microsoft Graph. Coerentemente con le altre offerte Copilot, le richieste, le risposte e i dati a cui si accede tramite Microsoft Graph non vengono usati per eseguire il training dei modelli di base.



Microsoft Learn: richieste, risposte e dati letti tramite Microsoft Graph non addestrano i modelli di base.

3.2 Copilot vede solo quello che vedi tu

Pensa a un collega appena assunto a cui dai le tue chiavi: può aprire i cassetti a cui hai accesso tu, non quelli del direttore. Copilot mostra solo i dati per cui hai almeno il permesso di visualizzazione. Se un file non è condiviso con te, Copilot non te lo mostra.

Microsoft Copilot visualizza solo i dati dell'organizzazione per i quali i singoli utenti dispongono almeno delle autorizzazioni di visualizzazione. È importante usare i modelli di autorizzazione disponibili nei servizi di Microsoft 365, come SharePoint, per garantire che gli utenti o i gruppi giusti abbiano l'accesso corretto ai contenuti giusti all'interno dell'organizzazione. Sono incluse le autorizzazioni concesse agli ute sterni all'organizzazione tramite soluzioni di collaborazione tra tenant, ad esempio i canali condivisi in Microsoft Teams.



Microsoft Learn: Copilot mostra solo i dati per cui hai almeno il permesso di visualizzazione.

3.3 Etichette di riservatezza e regole di conservazione

Copilot eredita le **etichette di riservatezza**, i bollini che dicono quanto è riservato un documento, e applica i **criteri di conservazione**, che stabiliscono per quanto tempo tenere i dati. Vale se l'azienda li ha impostati, e i controlli disponibili dipendono dall'abbonamento.

- **I controlli di accesso e i criteri si applicano a Copilot**: Copilot rispetta il modello di identità e le autorizzazioni, eredita le etichette di riservatezza, applica i criteri di conservazione, supporta il controllo delle interazioni e segue le impostazioni amministrative. I controlli e i criteri specifici varian conda del piano di abbonamento sottostante.



Microsoft Learn: etichette di riservatezza e criteri di conservazione valgono anche per Copilot; i controlli variano con il piano.

3.4 Contratto, GDPR e Data Boundary

L'uso di Copilot da parte delle organizzazioni è coperto dall'Addendum sulla protezione dei dati di Microsoft, con Microsoft come responsabile del trattamento. Gli impegni comprendono il supporto al GDPR, il regolamento europeo sulla privacy, e al Data

Boundary europeo, l'impegno a trattare i dati dei clienti europei all'interno dell'Unione Europea.

- **I tuoi dati sono privati:** Non useremo i tuoi dati se non come indicato da te. I nostri impegni in materia di privacy includono il supporto per il Regolamento generale sulla protezione dei dati (GDPR), il Limite dei dati dell'U… SO/IEC 27018 e il nostro Addendum sulla protezione dei dati.



Microsoft Learn: gli impegni sulla privacy comprendono il GDPR e il limite dei dati dell'UE.

> **FIN QUI, OTTIME NOTIZIE**
>
> Ma il diavolo si nasconde nei dettagli: il prossimo capitolo parla delle eccezioni a questi impegni.

4. Le zone grigie

Non lo dico per spaventarti: per usare bene uno strumento bisogna sapere come funziona davvero. Ecco quattro dettagli, più un adempimento che spesso si dimentica.

4.1 Le ricerche sul web

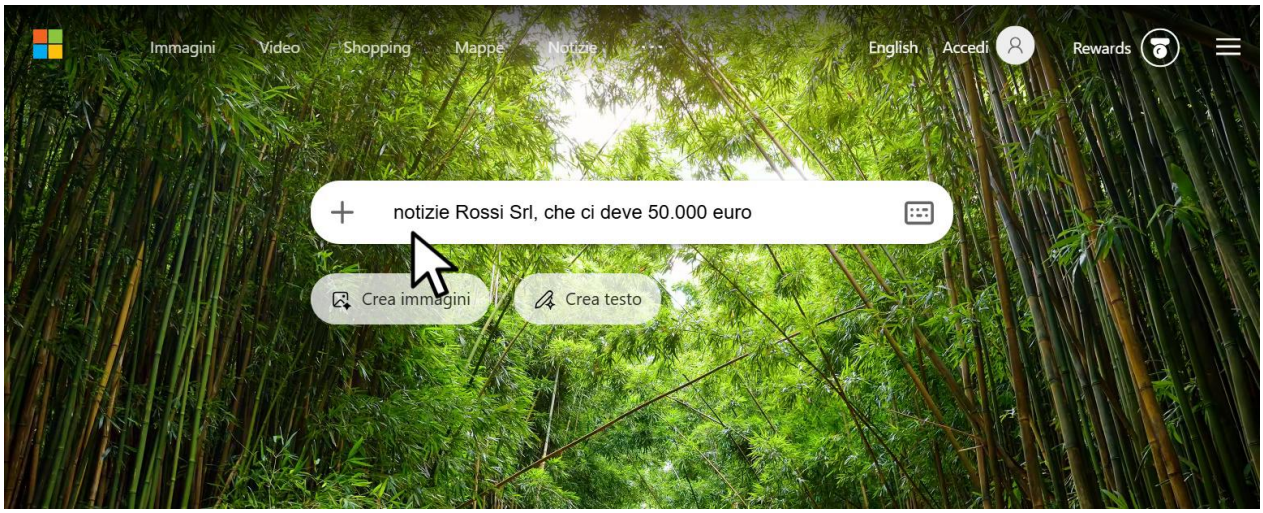
Quando serve un'informazione da internet, Copilot usa Bing, il motore di ricerca di Microsoft. Dalla tua richiesta ricava poche parole e le invia come ricerca. Queste ricerche **non rientrano** nell'impegno a restare in Europa e nemmeno nel contratto sulla protezione dei dati: seguono impegni separati, indicati nelle Condizioni del prodotto.

L'Addendum sulla protezione dei dati di Prodotti e Servizi Microsoft (DPA) non si applica all'uso di query di ricerca Web generate in Microsoft Copilot, Microsoft Copilot Chat o nel servizio di ricerca Bing. Inoltre, la conformi… IPAA e l'EU Data Boundary non si applicano alle query di ricerca generate.



Microsoft Learn: né il contratto sulla protezione dei dati né l'EU Data Boundary si applicano alle query di ricerca generate.

In pratica, se scrivi «cerca online notizie sulla Rossi Srl, che ci deve cinquantamila euro», quei dati possono uscire dal recinto. Microsoft spiega che l'identità dell'utente viene tolta dalla ricerca, ma viene inviato l'indirizzo IP per localizzare i risultati. La regola è semplice: niente dati riservati nelle ricerche.



Un esempio da evitare, scritto nella casella e non inviato: la Rossi Srl è inventata.

L'amministratore, cioè chi gestisce l'informatica dell'azienda, può disattivare le ricerche sul web per tutti o per alcuni gruppi con il criterio «Consenti ricerca Web in Copilot». Anche ogni utente di Microsoft 365 Copilot può spegnerle con l'interruttore «Contenuto Web», quando l'amministratore le lascia disponibili.

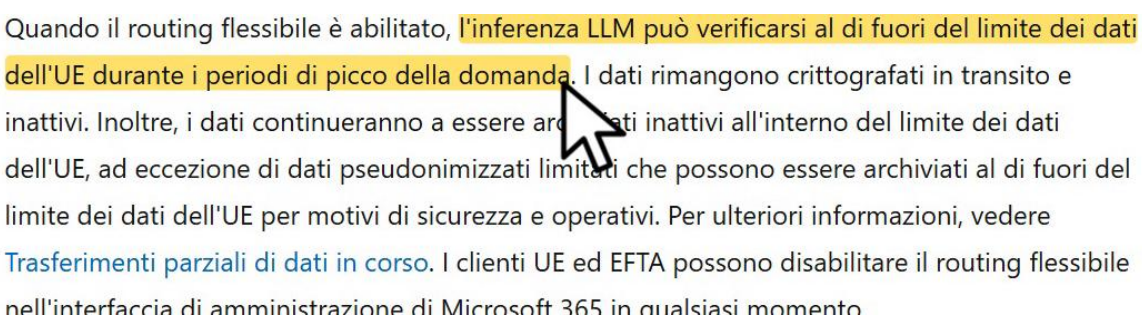
> Il modo principale in cui gli amministratori IT possono controllare l'accesso alla ricerca Web è usare il criterio **Consenti ricerca Web in Copilot** , disponibile solo nel servizio Cloud Policy per Microsoft 365. Questo criterio consente agli amministratori IT di attivare o disattivare la ricerca Web per utenti o gruppi di utenti nel tenant che gestiscono in base ai criteri dell'organizzazione, alle [illegible]i sulla privacy dei dati o ad altri requisiti normativi. Questo criterio si applica sia a Microsoft Copilot che a Microsoft Copilot Chat.

Microsoft Learn: l'amministratore può attivare o disattivare la ricerca web per utenti e gruppi.

4.2 L'ora di punta: il flex routing

Quando i server europei sono molto carichi, una parte dell'elaborazione può avvenire fuori dall'Unione Europea: secondo Microsoft, negli Stati Uniti, in Canada o in Australia. È come il corriere sotto Natale, che fa passare il tuo pacco da un magazzino più lontano perché quello vicino è pieno.

Si chiama **flex routing**, cioè percorso flessibile. I dati archiviati restano in Europa, salvo una quantità limitata di dati pseudonimizzati conservati per motivi di sicurezza e operativi: a spostarsi è l'elaborazione della risposta.


Quando il routing flessibile è abilitato, l'inferenza LLM può verificarsi al di fuori del limite dei dati dell'UE durante i periodi di picco della domanda. I dati rimangono crittografati in transito e inattivi. Inoltre, i dati continueranno a essere ar ati inattivi all'interno del limite dei dati dell'UE, ad eccezione di dati pseudonimizzati limitati che possono essere archiviati al di fuori del limite dei dati dell'UE per motivi di sicurezza e operativi. Per ulteriori informazioni, vedere Trasferimenti parziali di dati in corso. I clienti UE ed EFTA possono disabilitare il routing flessibile nell'interfaccia di amministrazione di Microsoft 365 in qualsiasi momento.

Microsoft Learn: con il routing flessibile attivo, nei picchi l'elaborazione può avvenire fuori dall'UE.

DA CONTROLLARE SUBITO

Microsoft indica che il routing flessibile è attivo in partenza per le aziende idonee create dopo il 25 marzo 2026. L'amministratore lo trova nell'interfaccia di amministrazione di Microsoft 365, in Copilot, Impostazioni, Visualizza tutto, e può scegliere di non consentirlo.


Configura il routing flessibile

Tutti gli amministratori tenant sono invitati a controllare l'impostazione di routing flessibile del tenant per assicurarsi che sia in li con i requisiti dell'azienda.

Microsoft Learn: gli amministratori sono invitati a controllare l'impostazione.

4.3 I modelli di intelligenza artificiale

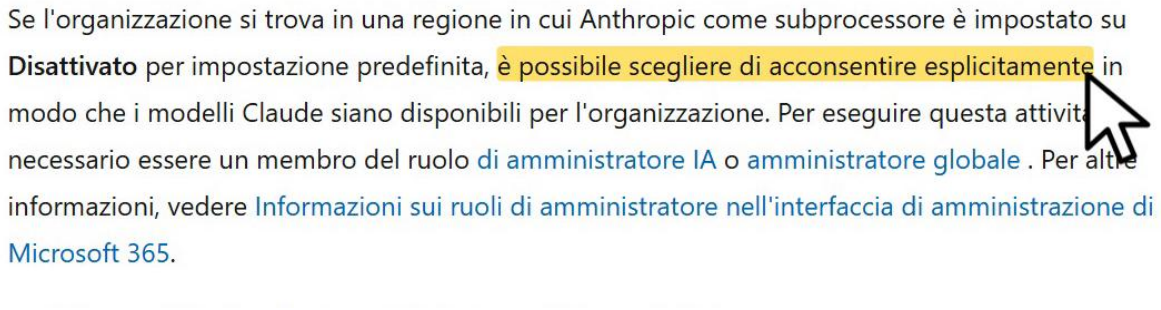
Copilot non ha un cervello suo: oggi può usare sia i modelli di OpenAI, la società di ChatGPT, sia i modelli Claude di Anthropic. I modelli Claude sono esclusi dall'impegno europeo sui dati, ed è per questo che nell'Unione Europea, nell'EFTA e nel Regno Unito sono disattivati in partenza.


ⓘ Importante

- I modelli Claude implementati nelle offerte Microsoft, ad esempio Microsoft Copilot, Researcher, Copilot Studio, Power Platform e Copilot nelle app Microsoft 365, sono attualmente esclusi dal limite dei dati dell'UE e, se applicabile, dagli impegni di elaborazione nel paese. I clienti all'interno del limite dei dati dell'UE e i clienti nel Regno Unito hanno i modelli Claude disabilitati per impostazione predefinita.
- Per informazioni sulla disponibilità dei modelli Claude nei cloud governativi li Stati Uniti (GCC, GCC High, DoD) e in altri cloud sovrani, vedere Aree di consenso esplicito ed esclusioni.

Microsoft Learn: i modelli Claude sono esclusi dal limite dei dati dell'UE e disattivati in partenza in Europa.

Non vuol dire che siano insicuri: di norma il contratto sulla protezione dei dati continua a valere e Anthropic opera come sub-responsabile di Microsoft. Cambiano le garanzie su dove vengono trattati i dati, quindi l'amministratore che li attiva deve farlo sapendolo.



Microsoft Learn: nelle regioni dove sono disattivati, l'organizzazione può scegliere di attivarli.

L'ECCEZIONE DA CONOSCERE

Alcuni modelli avanzati indicati come «modelli Anthropic con conservazione dei dati» seguono condizioni separate di Anthropic, non il contratto di Microsoft, e vanno abilitati a parte. Prima di attivarli serve una valutazione specifica.

4.4 L'oversharing: il rischio più importante

Oversharing significa condivisione eccessiva. Ricordi il collega nuovo che apre solo i cassetti a cui hai accesso tu? Ora immagina che negli anni, in azienda, qualcuno abbia lasciato aperti troppi cassetti: la cartella con gli stipendi condivisa con tutti per errore, il contratto riservato finito nella cartella comune.

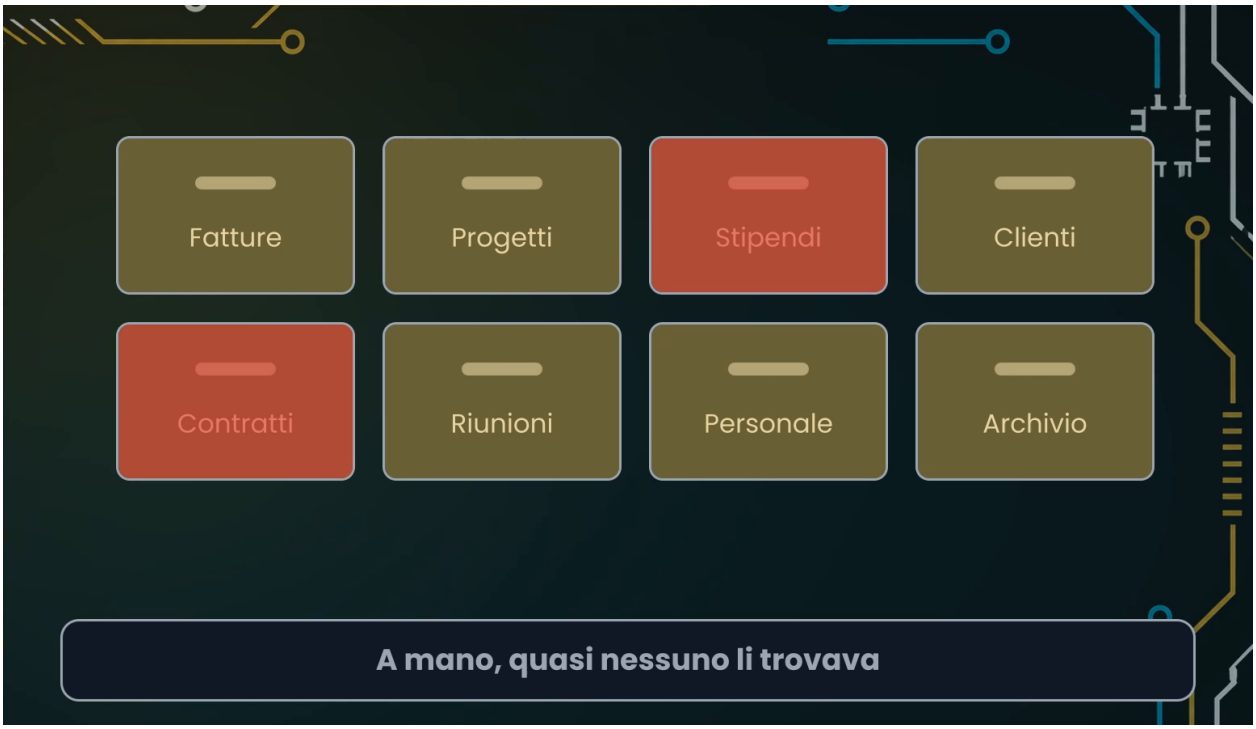
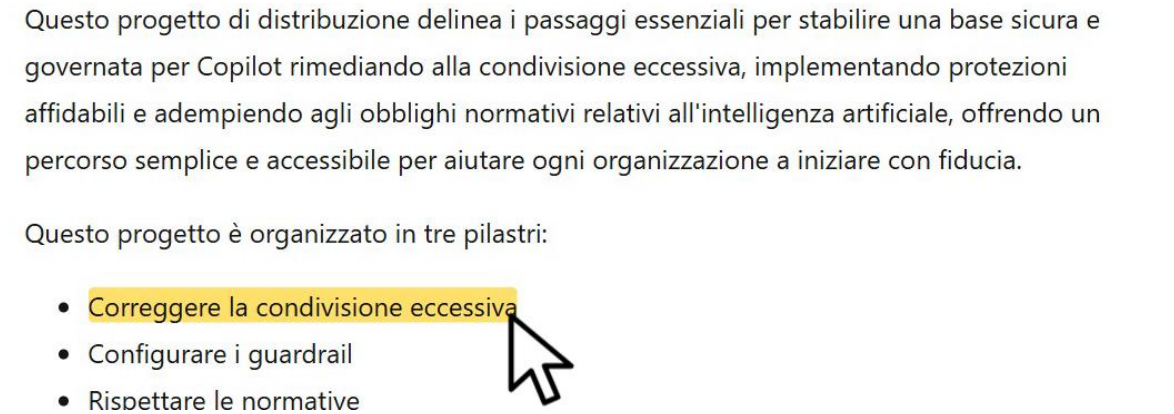


Illustrazione didattica: cartelle lasciate aperte, comprese quelle che non dovrebbero esserlo.

Finché bisognava cercarli a mano, quasi nessuno li trovava. Con Microsoft 365 Copilot basta una domanda innocente, tipo «riassumimi i documenti sul personale», e quei dati possono saltare fuori nella risposta. Copilot non crea il disordine: lo rende visibile. Non è un difetto del prodotto: rispetta i permessi, ma i permessi erano sbagliati.


Questo progetto di distribuzione delinea i passaggi essenziali per stabilire una base sicura e governata per Copilot rimediando alla condivisione eccessiva, implementando protezioni affidabili e adempiendo agli obblighi normativi relativi all'intelligenza artificiale, offrendo un percorso semplice e accessibile per aiutare ogni organizzazione a iniziare con fiducia.

Questo progetto è organizzato in tre pilastri:

- Correggere la condivisione eccessiva
- Configurare i guardrail
- Rispettare le normative

Microsoft Learn: la correzione della condivisione eccessiva è il primo pilastro della preparazione a Copilot.

4.5 La valutazione d'impatto

Introdurre Copilot in azienda spesso richiede una **valutazione d'impatto sulla protezione dei dati**, la cosiddetta DPIA: un'analisi scritta dei rischi per le persone, da fare prima di partire. È prevista dall'articolo 35 del GDPR per i trattamenti che possono presentare un rischio elevato. Coinvolgi chi si occupa di privacy in azienda.



5. La lista di controllo

Cinque punti, da appendere vicino alla macchinetta del caffè.

1. **Usa solo le versioni con l'account di lavoro** e cerca sempre lo scudo verde.
2. **Metti ordine nei cassetti** prima di attivare Copilot: controlla i permessi delle cartelle condivise, cioè chi può aprire cosa.
3. **Decidi in modo consapevole** se attivare i modelli Claude e se lasciare attivi le ricerche sul web e il flex routing, sapendo cosa cambia per i dati.
4. **Scrivi regole interne chiare**: cosa si può chiedere a Copilot e cosa no.
5. **Forma le persone**, il punto più importante: lo strumento più sicuro del mondo diventa rischioso in mano a chi non sa come funziona.

> **LA RISPOSTA IN UNA RIGA**
>
> Copilot è sicuro per la tua azienda? Sì, ma solo se è configurato bene e se le persone sanno usarlo.

Se vuoi capire se Copilot è lo strumento giusto per voi, oppure vuoi un corso per i tuoi colleghi su come usarlo bene e in sicurezza, faccio consulenza e formazione per aziende e professionisti, in presenza in Piemonte oppure online, senza legami con nessun fornitore. La prima chiacchierata conoscitiva è gratuita: trovi i contatti su gianlu.it.

Il controllo in venti minuti

Prova a fare questo controllo sul tuo ambiente di lavoro. Non servono dati riservati: se non hai i permessi per un punto, segnalo a chi gestisce l'informatica.

1. Apri Copilot e controlla con quale account sei entrato. Se usi quello di lavoro, cerca lo scudo verde.
2. Sfoglia le cartelle condivise a cui hai accesso e annota quelle che contengono documenti che non dovresti vedere. Non aprirli e segnalali al responsabile.
3. Chiedi all'amministratore tre risposte: le ricerche sul web sono attive? Il flex routing è consentito? I modelli Claude sono attivi?
4. Scrivi una richiesta di ricerca sul web su un tuo cliente immaginario, poi riscrivila togliendo nomi, importi e altri dati riservati.
5. Scrivi tre regole per i tuoi colleghi: una su che cosa si può chiedere, una su che cosa non si può incollare, una su a chi rivolgersi in caso di dubbio.

> **HAI FATTO UN BUON LAVORO SE**
>
> Sai dire quale versione di Copilot usi e con quale account.
>
> Hai un elenco delle cartelle da far controllare.
>
> Conosci le tre impostazioni della tua azienda, o sai chi può dirtele.
>
> Le tue tre regole stanno in poche righe e le capirebbe anche un collega appena assunto.

Le domande che arrivano in aula

Posso usare il Copilot gratuito per un documento di lavoro?

Per i dati dell'azienda no: le versioni personali non hanno le garanzie contrattuali pensate per le aziende. Usa la versione di lavoro con l'account aziendale.

Microsoft usa i miei documenti per addestrare l'intelligenza artificiale?

Nelle versioni di lavoro no: richieste, risposte e dati letti tramite Microsoft Graph non addestrano i modelli di base, secondo la documentazione di Microsoft.

I dati restano sempre in Europa?

Non sempre. Sono previste eccezioni per le ricerche web generate, per il flex routing se è consentito e per i modelli Claude se vengono attivati. Per questo vanno controllate le impostazioni.

Copilot può mostrarmi file che non dovrei vedere?

Mostra solo ciò per cui hai almeno il permesso di visualizzazione. Il problema nasce quando quel permesso è stato dato per errore: è l'oversharing.

La valutazione d'impatto è sempre obbligatoria?

L'articolo 35 del GDPR la richiede quando un trattamento può presentare un rischio elevato per le persone. Con Copilot succede spesso, ma la valutazione va fatta caso per caso con chi si occupa di privacy.

Glossario

Termine	Che cosa significa
Addendum sulla protezione dei dati (DPA)	La parte del contratto Microsoft che regola il trattamento dei dati dei clienti.
Copilot Chat	L'assistente a chat di Microsoft; con l'account di lavoro ha la protezione dei dati aziendali.
DPIA	Valutazione d'impatto sulla protezione dei dati: un'analisi dei rischi per le persone, prevista dall'articolo 35 del GDPR.
Etichetta di riservatezza	Il bollino che indica quanto è riservato un documento e quali regole si applicano.

Termine	Che cosa significa
EU Data Boundary	L'impegno di Microsoft a trattare i dati dei clienti europei all'interno dell'Unione Europea, con le eccezioni indicate.
Flex routing	Percorso flessibile: nei picchi di carico consente di elaborare le risposte fuori dall'Unione Europea.
GDPR	Il regolamento europeo sulla protezione dei dati personali.
Microsoft 365 Copilot	La versione a pagamento per le aziende, integrata nelle app e in grado di usare i dati di lavoro. Microsoft la sta rinominando Microsoft Copilot.
Microsoft Graph	Il sistema con cui Copilot raggiunge documenti, email e altri dati di lavoro a cui l'utente ha accesso.
Oversharing	Condivisione eccessiva: file e cartelle accessibili a più persone del necessario.

Per approfondire

Microsoft Learn: Protezione dei dati aziendali in Microsoft Copilot e Microsoft Copilot Chat - https://learn.microsoft.com/it-it/copilot/plan/enterprise-data-protection

Microsoft Learn: Dati, privacy e sicurezza per Microsoft Copilot - https://learn.microsoft.com/it-it/copilot/plan/microsoft-365-copilot-privacy

Microsoft Learn: Dati, privacy e sicurezza per la ricerca sul Web - https://learn.microsoft.com/it-it/copilot/plan/manage-public-web-access

Microsoft Learn: Routing flessibile (UE e EFTA) - https://learn.microsoft.com/it-it/copilot/manage/copilot-flex-routing

Microsoft Learn: Modelli Claude di Anthropic nei Microsoft Online Services - https://learn.microsoft.com/it-it/copilot/implement/connect-to-ai-subprocessor

Microsoft Learn: Panoramica di Microsoft Copilot - https://learn.microsoft.com/it-it/copilot/plan/copilot-overview

Microsoft Learn: Proteggere e gestire Microsoft Copilot, linee guida di base - https://learn.microsoft.com/it-it/copilot/plan/secure-govern-copilot-foundational-deployment-guidance

Garante per la protezione dei dati personali: Valutazione d'impatto della protezione dei dati (DPIA) - https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

Trinity College Dublin: guida a Copilot Chat e allo scudo verde - https://www.tcd.ie/itservices/our-services/microsoft-365-apps/copilot/copilot-chat/

Ramsac: lo scudo verde di Copilot spiegato - https://www.ramsac.com/blog/microsoft-copilot-green-shield-explained-a-simple-guide-for-uk-organisations/

ATTENZIONE

Dati verificati il 6 novembre 2026 sulla documentazione ufficiale, in parte tradotta automaticamente da Microsoft. Condizioni, nomi e impostazioni cambiano spesso: ricontrolla le fonti prima di decidere. Le informazioni hanno scopo formativo e non sostituiscono una consulenza legale.