Dati personali nei chatbot: cosa non dovresti mai incollare in una conversazione AI

Maria Cattini | 18/06/2026 | Intelligenza Artificiale

Il rischio più comune con i chatbot AI non è fare una domanda sbagliata.

È incollare troppo.

Un referto medico per farselo spiegare. Un contratto da riassumere. Una conversazione WhatsApp da interpretare. Una mail di lavoro con nomi, indirizzi e allegati. Un file aziendale. Un documento d'identità. Un elenco clienti. Una password "solo per farmi aiutare a capire se è sicura".

Il problema è che un chatbot non è un blocco note privato.

È un servizio digitale che può trattare, conservare, analizzare o usare le informazioni secondo regole diverse a seconda della piattaforma, dell'account, del piano, delle impostazioni privacy e delle funzioni attive. Alcuni servizi permettono di disattivare l'uso delle conversazioni per migliorare i modelli. Altri prevedono chat temporanee. Alcuni possono collegarsi ad app, file, email, calendario, browser o dispositivi.

La regola pratica è semplice: prima di incollare qualcosa in un chatbot, chiediti se saresti disposto a caricarlo su un servizio esterno di cui non controlli completamente conservazione, accessi, revisione e riuso.

Se la risposta è no, non incollarlo così com'è.

Perché i chatbot sembrano più privati di quanto siano

Una conversazione con un chatbot ha un aspetto intimo.

La finestra è personale, il tono è diretto, la risposta arriva come se ci fosse un assistente dedicato. Questo può far dimenticare che dietro quella finestra ci sono sistemi, policy, log, controlli di sicurezza, possibili revisioni, impostazioni di addestramento, servizi collegati e, in alcuni casi, conservazione della cronologia.

OpenAI, nella propria documentazione sui controlli dati, spiega che gli utenti possono disattivare l'opzione "Improve the model for everyone"; in quel caso le conversazioni restano nella cronologia, ma non vengono usate per addestrare ChatGPT. Le Temporary Chats, invece, non vengono salvate nella cronologia, non creano memorie e sono eliminate dai sistemi dopo 30 giorni, pur potendo essere esaminate per monitorare abusi.

Google, nel Privacy Hub di Gemini aggiornato al 19 maggio 2026, elenca tra i dati trattati prompt, file, schermate, foto, audio, video, contenuti generati, dati da app connesse, informazioni del dispositivo e, in alcune funzioni, contenuti dello schermo o del browser. Google avverte anche di non inserire informazioni confidenziali che non si vorrebbe fossero viste da un revisore o usate per migliorare i servizi.

Questi esempi non significano che tutti i chatbot funzionino nello stesso modo.

Significano il contrario: prima di usare un chatbot con dati sensibili bisogna capire quale servizio si sta usando, con quali impostazioni e dentro quale account.

Dati personali non significa solo codice fiscale

Molte persone pensano ai dati personali come a informazioni evidenti: nome, cognome, indirizzo, codice fiscale, numero di telefono, carta d’identità.

Sono dati personali, certo.

Ma non sono gli unici.

In una conversazione AI possono diventare personali anche:

• una storia clinica;
• una mail con riferimenti a colleghi o clienti;
• una chat familiare;
• una foto con volti, targhe o luoghi riconoscibili;
• un curriculum;
• un contratto;
• una fattura;
• un reclamo;
• una denuncia;
• una lista di utenti;
• un export da un gestionale;
• una tabella con dati pseudonimizzati ma facilmente ricollegabili a persone reali.

Il punto non è solo se nel testo compare il nome.

Il punto è se, leggendo quel contenuto, è possibile identificare una persona, ricostruire una situazione privata, dedurre informazioni sensibili o collegare dati che dovrebbero restare separati.

Un prompt può sembrare innocuo e contenere molto più di quanto pensiamo.

Cosa non dovresti mai incollare così com’è

Ci sono categorie di informazioni che non andrebbero inserite in un chatbot pubblico senza una valutazione seria, una base giuridica quando serve e, almeno, una forte minimizzazione.

1. Password, codici e credenziali

Non incollare password, token API, codici OTP, chiavi private, seed phrase, codici di recupero, link di reset o credenziali temporanee.

Nemmeno “solo per controllare”.

Un chatbot non serve a verificare se una password è sicura. Per quello esistono gestori di password, generatori locali e controlli specifici sulle violazioni note, da usare senza esporre la credenziale completa.

2. Documenti d’identità e dati finanziari

Evita carta d’identità, passaporto, patente, codice fiscale, IBAN, numeri di carta, buste paga, estratti conto, dichiarazioni fiscali e documenti assicurativi.

Se devi chiedere aiuto per capire un documento, rimuovi prima dati identificativi, numeri, codici, indirizzi, firme, QR code e riferimenti univoci.

3. Dati sanitari

Referti, diagnosi, prescrizioni, cartelle cliniche, dati genetici, terapie, informazioni psicologiche o immagini mediche sono dati estremamente delicati.

Un chatbot può aiutare a capire termini generali, ma non dovrebbe ricevere materiale sanitario personale non anonimizzato. Inoltre non va usato come sostituto di un medico. Se vuoi chiarire un termine, formula la domanda in modo generale.

Esempio più sicuro:

Che cosa significa in generale il termine “ipercolesterolemia” in un referto?

Evitare:

Ecco il mio referto completo con nome, data di nascita, valori, medico e struttura: spiegamelo.

4. Dati di altre persone

Non inserire conversazioni private, email, foto, dati di clienti, colleghi, studenti, pazienti, familiari o minori senza avere un motivo legittimo e senza ridurre al minimo le informazioni.

Questo è uno degli errori più frequenti: si pensa alla propria privacy, ma si caricano dati di altri.

Una chat di gruppo, una mail aziendale o una segnalazione interna possono contenere informazioni su persone che non hanno scelto di affidarle a un sistema AI.

5. Segreti aziendali e documenti interni

Evita business plan, contratti riservati, offerte commerciali, strategie, database clienti, roadmap di prodotto, incident report, codice proprietario, credenziali infrastrutturali, procedure interne e documenti soggetti a NDA.

Il problema non è solo la privacy.

È anche la sicurezza operativa.

Un documento interno può contenere nomi, ruoli, fornitori, sistemi usati, vulnerabilità, configurazioni, processi decisionali e dettagli che, messi insieme, diventano informazione sensibile.

6. Materiale legale o controversie in corso

Contratti, diffide, cause, denunce, lettere di avvocati, contenziosi di lavoro e documenti giudiziari vanno trattati con molta cautela.

Un chatbot può aiutare a capire parole generali, ma non sostituisce consulenza legale e non offre riservatezza professionale. Se devi ragionare su un tema, togli nomi, date, numeri di pratica, parti coinvolte e dettagli che rendono identificabile il caso.

Non basta cancellare il nome

Anonimizzare non significa sostituire “Mario Rossi” con “Persona A”.

Spesso una persona resta riconoscibile attraverso dettagli indiretti:

• ruolo;
• città;
• azienda;
• data;
• incarico;
• relazione familiare;
• cronologia degli eventi;
• importi;
• indirizzo;
• combinazione di più informazioni.

Esempio:

Il direttore amministrativo di una piccola azienda di Pescara, assunto a marzo 2025, ha ricevuto...

Anche senza nome, il profilo può essere identificabile da chi conosce il contesto.

La minimizzazione è più utile della finta anonimizzazione. Significa togliere tutto ciò che non serve alla domanda.

Se vuoi chiedere a un chatbot di aiutarti a migliorare una mail, non serve includere tutta la catena precedente. Se vuoi farti spiegare una clausola, non serve caricare l'intero contratto con nomi e firme. Se vuoi riassumere una tabella, non serve inserire dati individuali quando basta una versione aggregata.

Una versione più sicura dello stesso prompt

Il metodo pratico è trasformare il dato personale in scenario generale.

Prompt rischioso:

Questa è la mail del mio cliente con nome, numero di telefono, indirizzo, preventivo e problema tecnico. Scrivi una risposta.

Prompt migliore:

Aiutami a scrivere una risposta professionale a un cliente che segnala un ritardo nella consegna. Tono: cortese, chiaro, senza ammettere responsabilità non verificate. Includi una promessa di aggiornamento entro 24 ore.

Prompt rischioso:

Ecco il contratto firmato con la società X: dimmi se posso uscirne senza penali.

Prompt migliore:

Spiegami in termini generali quali elementi controllare in una clausola di recesso di un contratto commerciale. Non fare consulenza legale, dammi una checklist da discutere con un professionista.

Prompt rischioso:

Ecco la chat completa con un dipendente: dimmi se posso licenziarlo.

Prompt migliore:

Quali aspetti generali dovrebbe valutare un'azienda prima di prendere decisioni disciplinari su un comportamento online? Indica limiti, documentazione e necessità di consulenza legale.

Il chatbot resta utile.

Ma non riceve più tutto il contesto sensibile.

Controlla le impostazioni, ma non affidarti solo alle impostazioni

Le impostazioni privacy sono importanti.

Se usi ChatGPT, controlla i Data Controls: puoi disattivare l'uso delle conversazioni per migliorare il modello e usare chat temporanee quando non vuoi salvare una conversazione nella cronologia. Se usi Gemini, controlla Gemini Apps Activity, app connesse, permessi del dispositivo, eventuale accesso a contenuti dello schermo, browser, file o servizi Google.

Ma le impostazioni non sostituiscono il criterio.

Anche una chat temporanea non trasforma un chatbot in uno spazio coperto da segreto professionale. Anche un opt-out dall'addestramento non significa che il servizio non debba trattare dati per funzionare, prevenire abusi, rispettare obblighi legali o garantire sicurezza. Anche un piano business può avere condizioni più adatte al lavoro, ma va letto e configurato.

La regola migliore resta: non inserire ciò che non è necessario.

Cosa fare in azienda

Per un uso professionale, il problema non può essere lasciato alla buona volontà dei singoli.

Serve una regola interna chiara:

• quali strumenti AI sono autorizzati;
• quali dati possono essere inseriti;
• quali dati sono vietati;
• chi può usare account personali e chi solo account aziendali;
• come anonimizzare i contenuti;
• quando usare strumenti con protezioni enterprise;
• come gestire file, allegati e screenshot;
• come documentare l'uso dell'AI in processi sensibili.

Una policy troppo lunga non verrà letta. Meglio una checklist breve, concreta, con esempi.

Esempio:

Non inserire: password, dati sanitari, dati di clienti, documenti interni integrali, contratti firmati, dati di minori, segreti commerciali. Puoi inserire: testi riscritti senza dati personali, scenari generali, bozze non riservate, domande tecniche senza credenziali, dati aggregati.

Questo non elimina tutti i rischi.

Ma riduce gli errori più prevedibili.

Checklist prima di premere Invio

Prima di inviare un prompt a un chatbot, chiediti:

• contiene nomi, indirizzi, numeri di telefono, email o codici identificativi?
• contiene dati sanitari, finanziari, legali o di minori?
• contiene dati di clienti, colleghi, dipendenti o familiari?

• contiene password, token, credenziali o link di accesso?
• contiene segreti aziendali, codice proprietario o documenti interni?
• posso ottenere lo stesso risultato usando uno scenario generale?
• posso rimuovere nomi, date, luoghi, importi e riferimenti univoci?
• sto usando un account personale o aziendale?
• ho controllato impostazioni privacy, cronologia, memoria e app collegate?
• sarei tranquillo se quel contenuto fosse letto da un revisore autorizzato del servizio?

Se una risposta ti mette a disagio, fermati.

Riscrivi il prompt.

La regola finale: meno contesto sensibile, più metodo

I chatbot sono utili quando aiutano a ragionare, sintetizzare, scrivere, tradurre, organizzare e controllare.

Diventano rischiosi quando li trattiamo come contenitori neutri di qualsiasi informazione.

La soluzione non è smettere di usarli.

È usarli con meno automatismo.

Prima di incollare un documento, chiediti che cosa vuoi ottenere. Poi togli tutto ciò che non serve a quel risultato. Trasforma dati personali in esempi generali. Sostituisci documenti completi con estratti puliti. Usa checklist invece di caricare casi reali. Controlla impostazioni, memoria, cronologia e app collegate.

Un buon prompt non è quello che consegna tutto al modello.

È quello che dà abbastanza contesto per ottenere aiuto senza regalare dati che non dovevano uscire da lì.
Il rischio più comune con i chatbot AI non è fare una domanda sbagliata.

È incollare troppo.

Un referto medico per farselo spiegare. Un contratto da riassumere. Una conversazione WhatsApp da interpretare. Una mail di lavoro con nomi, indirizzi e allegati. Un file aziendale. Un documento d’identità. Un elenco clienti. Una password “solo per farmi aiutare a capire se è sicura”.

Il problema è che un chatbot non è un blocco note privato.

È un servizio digitale che può trattare, conservare, analizzare o usare le informazioni secondo regole diverse a seconda della piattaforma, dell’account, del piano, delle impostazioni privacy e delle funzioni attive. Alcuni servizi permettono di disattivare l’uso delle conversazioni per migliorare i modelli. Altri prevedono chat temporanee. Alcuni possono collegarsi ad app, file, email, calendario, browser o dispositivi.

La regola pratica è semplice: prima di incollare qualcosa in un chatbot, chiediti se saresti disposto a caricarlo su un servizio esterno di cui non controlli completamente conservazione, accessi, revisione e riuso.

Se la risposta è no, non incollarlo così com’è.

Perché i chatbot sembrano più privati di quanto siano

Una conversazione con un chatbot ha un aspetto intimo.

La finestra è personale, il tono è diretto, la risposta arriva come se ci fosse un assistente dedicato. Questo può far dimenticare che dietro quella finestra ci sono sistemi, policy, log, controlli di sicurezza, possibili revisioni, impostazioni di addestramento, servizi collegati e, in alcuni casi, conservazione della cronologia.

OpenAI, nella propria documentazione sui controlli dati, spiega che gli utenti possono disattivare l'opzione "Improve the model for everyone"; in quel caso le conversazioni restano nella cronologia, ma non vengono usate per addestrare ChatGPT. Le Temporary Chats, invece, non vengono salvate nella cronologia, non creano memorie e sono eliminate dai sistemi dopo 30 giorni, pur potendo essere esaminate per monitorare abusi.

Google, nel Privacy Hub di Gemini aggiornato al 19 maggio 2026, elenca tra i dati trattati prompt, file, schermate, foto, audio, video, contenuti generati, dati da app connesse, informazioni del dispositivo e, in alcune funzioni, contenuti dello schermo o del browser. Google avverte anche di non inserire informazioni confidenziali che non si vorrebbe fossero viste da un revisore o usate per migliorare i servizi.

Questi esempi non significano che tutti i chatbot funzionino nello stesso modo.

Significano il contrario: prima di usare un chatbot con dati sensibili bisogna capire quale servizio si sta usando, con quali impostazioni e dentro quale account.

Dati personali non significa solo codice fiscale

Molte persone pensano ai dati personali come a informazioni evidenti: nome, cognome, indirizzo, codice fiscale, numero di telefono, carta d'identità.

Sono dati personali, certo.

Ma non sono gli unici.

In una conversazione AI possono diventare personali anche:

• una storia clinica;
• una mail con riferimenti a colleghi o clienti;
• una chat familiare;
• una foto con volti, targhe o luoghi riconoscibili;
• un curriculum;
• un contratto;
• una fattura;
• un reclamo;
• una denuncia;
• una lista di utenti;
• un export da un gestionale;
• una tabella con dati pseudonimizzati ma facilmente ricollegabili a persone reali.

Il punto non è solo se nel testo compare il nome.

Il punto è se, leggendo quel contenuto, è possibile identificare una persona, ricostruire una situazione privata, dedurre informazioni sensibili o collegare dati che dovrebbero restare separati.

Un prompt può sembrare innocuo e contenere molto più di quanto pensiamo.

Cosa non dovresti mai incollare così com'è

Ci sono categorie di informazioni che non andrebbero inserite in un chatbot pubblico senza una valutazione seria, una base giuridica quando serve e, almeno, una forte minimizzazione.

1. Password, codici e credenziali

Non incollare password, token API, codici OTP, chiavi private, seed phrase, codici di recupero, link di reset o credenziali temporanee.

Nemmeno “solo per controllare”.

Un chatbot non serve a verificare se una password è sicura. Per quello esistono gestori di password, generatori locali e controlli specifici sulle violazioni note, da usare senza esporre la credenziale completa.

2. Documenti d’identità e dati finanziari

Evita carta d’identità, passaporto, patente, codice fiscale, IBAN, numeri di carta, buste paga, estratti conto, dichiarazioni fiscali e documenti assicurativi.

Se devi chiedere aiuto per capire un documento, rimuovi prima dati identificativi, numeri, codici, indirizzi, firme, QR code e riferimenti univoci.

3. Dati sanitari

Referti, diagnosi, prescrizioni, cartelle cliniche, dati genetici, terapie, informazioni psicologiche o immagini mediche sono dati estremamente delicati.

Un chatbot può aiutare a capire termini generali, ma non dovrebbe ricevere materiale sanitario personale non anonimizzato. Inoltre non va usato come sostituto di un medico. Se vuoi chiarire un termine, formula la domanda in modo generale.

Esempio più sicuro:

Che cosa significa in generale il termine “ipercolesterolemia” in un referto?

Evitare:

Ecco il mio referto completo con nome, data di nascita, valori, medico e struttura: spiegamelo.

4. Dati di altre persone

Non inserire conversazioni private, email, foto, dati di clienti, colleghi, studenti, pazienti, familiari o minori senza avere un motivo legittimo e senza ridurre al minimo le informazioni.

Questo è uno degli errori più frequenti: si pensa alla propria privacy, ma si caricano dati di altri.

Una chat di gruppo, una mail aziendale o una segnalazione interna possono contenere informazioni su persone che non hanno scelto di affidarle a un sistema AI.

5. Segreti aziendali e documenti interni

Evita business plan, contratti riservati, offerte commerciali, strategie, database clienti, roadmap di prodotto, incident report, codice proprietario, credenziali infrastrutturali, procedure interne e documenti soggetti a NDA.

Il problema non è solo la privacy.

È anche la sicurezza operativa.

Un documento interno può contenere nomi, ruoli, fornitori, sistemi usati, vulnerabilità, configurazioni, processi decisionali e dettagli che, messi insieme, diventano informazione sensibile.

6. Materiale legale o controversie in corso

Contratti, diffide, cause, denunce, lettere di avvocati, contenziosi di lavoro e documenti giudiziari vanno trattati con molta cautela.

Un chatbot può aiutare a capire parole generali, ma non sostituisce consulenza legale e non offre riservatezza professionale. Se devi ragionare su un tema, togli nomi, date, numeri di pratica, parti coinvolte e dettagli che rendono identificabile il caso.

Non basta cancellare il nome

Anonimizzare non significa sostituire “Mario Rossi” con “Persona A”.

Spesso una persona resta riconoscibile attraverso dettagli indiretti:

• ruolo;
• città;
• azienda;
• data;
• incarico;
• relazione familiare;
• cronologia degli eventi;
• importi;
• indirizzo;
• combinazione di più informazioni.

Esempio:

Il direttore amministrativo di una piccola azienda di Pescara, assunto a marzo 2025, ha ricevuto...

Anche senza nome, il profilo può essere identificabile da chi conosce il contesto.

La minimizzazione è più utile della finta anonimizzazione. Significa togliere tutto ciò che non serve alla domanda.

Se vuoi chiedere a un chatbot di aiutarti a migliorare una mail, non serve includere tutta la catena precedente. Se vuoi farti spiegare una clausola, non serve caricare l’intero contratto con nomi e firme. Se vuoi riassumere una tabella, non serve inserire dati individuali quando basta una versione aggregata.

Una versione più sicura dello stesso prompt

Il metodo pratico è trasformare il dato personale in scenario generale.

Prompt rischioso:

Questa è la mail del mio cliente con nome, numero di telefono, indirizzo, preventivo e problema tecnico. Scrivi una risposta.

Prompt migliore:

Aiutami a scrivere una risposta professionale a un cliente che segnala un ritardo nella consegna. Tono: cortese, chiaro, senza ammettere responsabilità non verificate. Includi una promessa di aggiornamento entro 24 ore.

Prompt rischioso:

Ecco il contratto firmato con la società X: dimmi se posso uscirne senza penali.

Prompt migliore:

Spiegami in termini generali quali elementi controllare in una clausola di recesso di un contratto commerciale. Non fare consulenza legale, dammi una checklist da discutere con un professionista.

Prompt rischioso:

Ecco la chat completa con un dipendente: dimmi se posso licenziarlo.

Prompt migliore:

Quali aspetti generali dovrebbe valutare un’azienda prima di prendere decisioni disciplinari su un comportamento online? Indica limiti, documentazione e necessità di consulenza legale.

Il chatbot resta utile.

Ma non riceve più tutto il contesto sensibile.

Controlla le impostazioni, ma non affidarti solo alle impostazioni

Le impostazioni privacy sono importanti.

Se usi ChatGPT, controlla i Data Controls: puoi disattivare l’uso delle conversazioni per migliorare il modello e usare chat temporanee quando non vuoi salvare una conversazione nella cronologia. Se usi Gemini, controlla Gemini Apps Activity, app connesse, permessi del dispositivo, eventuale accesso a contenuti dello schermo, browser, file o servizi Google.

Ma le impostazioni non sostituiscono il criterio.

Anche una chat temporanea non trasforma un chatbot in uno spazio coperto da segreto professionale. Anche un opt-out dall’addestramento non significa che il servizio non debba trattare dati per funzionare, prevenire abusi, rispettare obblighi legali o garantire sicurezza. Anche un piano business può avere condizioni più adatte al lavoro, ma va letto e configurato.

La regola migliore resta: non inserire ciò che non è necessario.

Cosa fare in azienda

Per un uso professionale, il problema non può essere lasciato alla buona volontà dei singoli.

Serve una regola interna chiara:

• quali strumenti AI sono autorizzati;
• quali dati possono essere inseriti;
• quali dati sono vietati;
• chi può usare account personali e chi solo account aziendali;
• come anonimizzare i contenuti;
• quando usare strumenti con protezioni enterprise;
• come gestire file, allegati e screenshot;
• come documentare l’uso dell’AI in processi sensibili.

Una policy troppo lunga non verrà letta. Meglio una checklist breve, concreta, con esempi.

Esempio:

Non inserire: password, dati sanitari, dati di clienti, documenti interni integrali, contratti firmati, dati

di minori, segreti commerciali. Puoi inserire: testi riscritti senza dati personali, scenari generali, bozze non riservate, domande tecniche senza credenziali, dati aggregati.

Questo non elimina tutti i rischi.

Ma riduce gli errori più prevedibili.

Checklist prima di premere Invio

Prima di inviare un prompt a un chatbot, chiediti:

• contiene nomi, indirizzi, numeri di telefono, email o codici identificativi?
• contiene dati sanitari, finanziari, legali o di minori?
• contiene dati di clienti, colleghi, dipendenti o familiari?
• contiene password, token, credenziali o link di accesso?
• contiene segreti aziendali, codice proprietario o documenti interni?
• posso ottenere lo stesso risultato usando uno scenario generale?
• posso rimuovere nomi, date, luoghi, importi e riferimenti univoci?
• sto usando un account personale o aziendale?
• ho controllato impostazioni privacy, cronologia, memoria e app collegate?
• sarei tranquillo se quel contenuto fosse letto da un revisore autorizzato del servizio?

Se una risposta ti mette a disagio, fermati.

Riscrivi il prompt.

La regola finale: meno contesto sensibile, più metodo

I chatbot sono utili quando aiutano a ragionare, sintetizzare, scrivere, tradurre, organizzare e controllare.

Diventano rischiosi quando li trattiamo come contenitori neutri di qualsiasi informazione.

La soluzione non è smettere di usarli.

È usarli con meno automatismo.

Prima di incollare un documento, chiediti che cosa vuoi ottenere. Poi togli tutto ciò che non serve a quel risultato. Trasforma dati personali in esempi generali. Sostituisci documenti completi con estratti puliti. Usa checklist invece di caricare casi reali. Controlla impostazioni, memoria, cronologia e app collegate.

Un buon prompt non è quello che consegna tutto al modello.

È quello che dà abbastanza contesto per ottenere aiuto senza regalare dati che non dovevano uscire da lì.