ChatGPT

Deep Research – Privacy e Protezione Dati di ChatGPT Enterprise

Proprietà dei dati e riservatezza in ChatGPT Enterprise

ChatGPT Enterprise è progettato per garantire che i dati della tua organizzazione rimangano sotto il tuo controllo. I testi o file che inserisci (input) e le risposte generate (output) **rimangono di tua proprietà**: OpenAI **non utilizza i dati aziendali per addestrare i propri modelli di AI** a meno che tu non lo consenta esplicitamente [1]. In altre parole, ciò che condividi con ChatGPT Enterprise **resta privato** della tua azienda e non viene impiegato per migliorare il sistema o condiviso con altri utenti. Inoltre, l'azienda può **decidere per quanto tempo conservare le conversazioni** su ChatGPT Enterprise, impostando periodi di **retention** (conservazione) dei dati o la cancellazione automatica, così da rispettare le proprie policy interne [1].

Esempio pratico: un dipendente chiede a ChatGPT Enterprise di riassumere un protocollo clinico interno. La bozza generata **resta nei confini aziendali**: l'azienda **mantiene tutti i diritti** sul testo inserito e su quello generato, e OpenAI **non lo riutilizza** per altri scopi [1]. Questo significa che informazioni sensibili (come strategie di ricerca o dati non pubblici) non diventano parte del patrimonio di conoscenza di OpenAI, ma restano confidenziali.

Fonte: OpenAI – *Enterprise privacy commitments* (openai.com, aggiornato giugno 2025) [1]

Sicurezza dei dati ed esclusione degli accessi non autorizzati

OpenAI adotta **misure di sicurezza avanzate** per proteggere i dati forniti a ChatGPT Enterprise. Tutti i contenuti sono **crittografati** sia durante la trasmissione sia quando vengono archiviati sui server di OpenAI [2]. In pratica, ogni messaggio inviato o ricevuto viaggia in forma illeggibile a terzi (cifratura TLS) e viene conservato in modo cifrato (AES-256) sui sistemi di OpenAI [2]. Questo garantisce che, anche intercettando il traffico o accedendo ai server, **nessuno possa leggere i dati** senza la chiave di decrittazione.

Anche l'**accesso ai dati** è strettamente controllato. All'interno dell'azienda, **solo gli utenti autorizzati** possono utilizzare ChatGPT Enterprise tramite le credenziali aziendali (es. login Single Sign-On aziendale); inoltre, gli amministratori IT possono gestire permessi e funzionalità disponibili per ciascun gruppo di utenti [3]. Dal lato di OpenAI, **solo personale autorizzato** può accedere ai dati delle conversazioni, e solo in casi eccezionali (ad esempio per risolvere un incidente tecnico, su richiesta esplicita dell'azienda, o per obblighi legali) [4]. Queste misure assicurano che i contenuti scambiati con ChatGPT Enterprise **non siano visibili né utilizzabili da persone non autorizzate**.

Esempio pratico: un ricercatore condivide dati riservati di laboratorio con ChatGPT Enterprise per ottenere un'analisi. Durante l'intero processo, i dati **viaggiano cifrati** e possono essere letti solo dal ricercatore stesso. Gli amministratori aziendali hanno la possibilità di verificare l'attività (audit log) ma **nessun estraneo può accedere** a queste informazioni. Anche in caso di necessità di supporto tecnico, OpenAI potrà vedere questi dati solo previa autorizzazione esplicita dell'azienda e seguendo procedure di sicurezza rigorose [4].

Fonti: OpenAI – *Enterprise privacy FAQ* (openai.com, 2025) [2] [4]

Conformità a normative (GDPR etc.) e certificazioni di sicurezza

ChatGPT Enterprise è allineato alle principali **normative sulla protezione dei dati**. OpenAI ha dichiarato che le sue pratiche rispettano leggi come il GDPR (Regolamento Generale sulla Protezione dei Dati per l'UE) e il CCPA (legge sulla privacy per la California) [5]. Per i clienti, ciò significa che l'uso di ChatGPT Enterprise può essere configurato in modo da **supportare la conformità legale**, ad esempio rispettando i diritti degli interessati e minimizzando la conservazione dei dati personali.

Inoltre, OpenAI ha ottenuto **certificazioni di sicurezza indipendenti** che attestano l'affidabilità dei controlli interni. In particolare, ChatGPT Enterprise è coperto da un audit **SOC 2 Type 2** superato con successo [5]. Questa certificazione – rilasciata dopo verifica da parte di auditor terzi – conferma che OpenAI adotta standard industriali rigorosi in materia di **sicurezza, riservatezza e integrità dei dati** nelle sue piattaforme. All'atto pratico, per un'azienda ciò offre una garanzia aggiuntiva: un ente indipendente ha controllato che le misure di sicurezza dichiarate da OpenAI siano effettivamente in atto e funzionanti.

OpenAI fornisce anche opzioni di **data residency** (residenza dei dati) per aiutare le organizzazioni a rispettare vincoli locali. Ad esempio, i clienti ChatGPT Enterprise possono richiedere che i dati siano archiviati solo in specifiche regioni (come nell'Unione Europea) per ottemperare a requisiti di **sovranità dei dati** locali [5]. Questo è particolarmente rilevante per le aziende farmaceutiche multinazionali che devono garantire che i dati dei pazienti o i dati clinici non escano da determinati territori.

Esempio pratico: una casa farmaceutica con sede in Europa adotta ChatGPT Enterprise per i propri dipendenti. Grazie alle funzionalità offerte, l'azienda imposta la **localizzazione dei dati in UE** per tutte le conversazioni, assicurando che informazioni personali (es. dati di sperimentazioni cliniche europee) **non vengano archiviate su server fuori dall'Europa**. Inoltre, l'azienda verifica che OpenAI abbia le **certificazioni di sicurezza** adeguate (come SOC 2) e quindi può riferire agli auditor interni che il fornitore AI risponde agli standard di settore [5].

Fonte: OpenAI – *ChatGPT Enterprise – Security & compliance* (openai.com, 2025) [5]

Supporto dedicato e garanzie contrattuali offerte da OpenAI

Per ulteriore tranquillità, OpenAI offre **accordi contrattuali specifici** ai clienti ChatGPT Enterprise in merito al trattamento e alla protezione dei dati. In particolare, un'azienda può sottoscrivere con OpenAI un **Data Processing Addendum (DPA)** – un **accordo sul trattamento dei dati** – che definisce in modo vincolante come OpenAI gestirà i dati della tua organizzazione in conformità alle leggi sulla privacy (ad esempio il GDPR) [6]. Attraverso il DPA, OpenAI si impegna legalmente a **utilizzare i dati solo per erogare il servizio**, a non conservarli più del necessario e ad adottare tutte le misure di sicurezza e riservatezza previste. L'azienda cliente ottiene così garanzie contrattuali aggiuntive oltre alle policy standard.

Nel caso in cui la tua azienda tratti **dati sanitari sensibili** (ad esempio informazioni su pazienti, cartelle cliniche o altre informazioni coperte da normative sulla salute), OpenAI è disponibile a firmare un **Business Associate Agreement (BAA)**. Si tratta di un accordo richiesto dalla legge statunitense HIPAA per i fornitori che gestiscono **dati medici protetti**, e OpenAI ha dichiarato di poter stipulare BAA a supporto della conformità dei clienti in ambito sanitario [7]. Questo può essere rilevante se una

azienda farmaceutica utilizza ChatGPT Enterprise anche per attività collegate a dati clinici o studi medici soggetti a HIPAA o standard equivalenti.

ChatGPT Enterprise include anche un **supporto tecnico dedicato** per i clienti business. OpenAI offre assistenza **24 ore su 24, 7 giorni su 7**, con **SLA** (Service Level Agreement, tempi di risposta garantiti) per risolvere tempestivamente eventuali problemi [8]. Inoltre, i clienti Enterprise possono richiedere **supporto premium**, ottenendo referenti tecnici dedicati e disponibilità on-call, cioè specialisti pronti a intervenire per esigenze specifiche [8]. In pratica, ciò significa che la tua azienda non è mai "sola": per qualsiasi dubbio su sicurezza, configurazione o emergenza legata a ChatGPT, c'è un canale prioritario con OpenAI a disposizione.

Esempio pratico: prima di iniziare a usare ChatGPT Enterprise sui dati di un nuovo trial clinico, una società farmaceutica firma il **DPA** con OpenAI, assicurandosi per iscritto che i dati dei pazienti saranno trattati secondo GDPR e solo per fornire il servizio [6]. In aggiunta, l'azienda verifica con OpenAI la possibilità di un **BAA** perché prevede di gestire dati sanitari negli Stati Uniti [7]. Durante l'uso del prodotto, se i ricercatori hanno un problema (ad esempio una difficoltà tecnica o una domanda sulla sicurezza), sanno di poter contattare il **supporto Enterprise** di OpenAI in qualsiasi momento, ottenendo aiuto rapido grazie al canale dedicato attivo 24/7.

Fonti: OpenAI – *Enterprise privacy FAQ* (DPA) [6]; *OpenAI API compliance* (BAA, 2025) [7]; OpenAI – *ChatGPT Enterprise Overview* (supporto, 2023) [8]

Rischi residui e misure preventive per un'azienda farmaceutica

Nonostante le robuste protezioni fornite da ChatGPT Enterprise, restano alcuni **rischi potenziali** da tenere presenti, specialmente in un'azienda farmaceutica. Di seguito evidenziamo i principali rischi residui in parole semplici e le **azioni preventive** consigliate per mitigarli:

- **Condivisione di dati sensibili:** Se un utente inserisce nel prompt di ChatGPT informazioni personali di pazienti o segreti industriali, quei dati escono dal controllo diretto dell'azienda (anche se vengono protetti da OpenAI) [9]. *Misura preventiva:* **Evitare di inserire dati altamente sensibili** a meno che non sia strettamente necessario. Ad esempio, **non copiare nomi di pazienti, dettagli di identificazione o formule riservate** nelle richieste. Se proprio devi discutere un caso reale, **anonimizza i dati** (es. usa iniziali invece di nomi completi, valori approssimati invece di dati esatti) così che le informazioni personali o critiche non vengano esposte.

- **Accuratezza delle risposte ("allucinazioni"):** ChatGPT può generare risposte che **sembrano autorevoli ma possono contenere errori o informazioni inventate** [10]. Questo è un rischio se l'output viene utilizzato senza verifica, specialmente in ambito scientifico o normativo dove l'accuratezza è cruciale. *Misura preventiva:* **Verificare sempre le informazioni importanti** fornite da ChatGPT. In pratica, **non prendere mai le risposte come verità assoluta**. Se ChatGPT, ad esempio, riassume i risultati di uno studio clinico, fai controllare il riassunto da un esperto interno o confrontalo con la pubblicazione originale. Ogni volta che l'AI fornisce un dato critico (es. dosaggio di un farmaco, norma regolatoria, risultato scientifico), **conferma quel dato su fonti ufficiali** o con un collega qualificato prima di utilizzarlo [11].

- **Contesto regolatorio e validazione:** In un settore fortemente regolamentato come il farmaceutico, utilizzare testi generati dall'AI senza la dovuta cautela può portare a problemi di **non-conformità normativa**. Ad esempio, inserire parti non verificate di testo generate da

ChatGPT in un documento da sottoporre alle autorità regolatorie (EMA, AIFA, FDA, ecc.) potrebbe violare le linee guida di documentazione o qualità [12]. *Misura preventiva:* **Usa ChatGPT come strumento di supporto, non come fonte finale.** Ogni contenuto destinato a documentazione ufficiale o comunicazione esterna **deve essere attentamente revisionato**. Assicurati che **un esperto umano approvi e convalidi** qualsiasi informazione generata dall'AI prima dell'uso ufficiale [13]. Ad esempio, se ChatGPT ti aiuta a redigere una relazione di farmacovigilanza, fai in modo che il responsabile di area la riveda integralmente, verificando dati e tono, per garantire che rispetti tutte le normative e standard interni.

- **Proprietà intellettuale e copyright:** ChatGPT genera testi attingendo alle conoscenze apprese da enormi quantità di dati pubblici. C'è quindi il rischio (seppur remoto) che una risposta includa **frasi o estratti protetti da copyright** o che rielabori contenuti tratti da terzi senza citarli [14]. Per un'azienda farmaceutica, questo potrebbe tradursi in uso involontario di materiale non autorizzato (ad esempio descrizioni tratte da brevetti altrui o da articoli scientifici coperti da diritto d'autore). *Misura preventiva:* **Tratta sempre l'output di ChatGPT come una bozza da controllare.** Prima di diffondere esternamente un testo generato, sottoponilo a una **revisione per escludere plagi o riferimenti non consentiti**. Evita di incollare direttamente nelle richieste testi da documenti interni coperti da diritti esclusivi, a meno di reali necessità, e comunque dopo aver valutato i rischi. In sintesi, **usa l'AI per ispirazione o aiuto, ma verifica che il risultato finale sia originale e conforme alle politiche su IP** dell'azienda.

Fonti (rischi): ISPE *Pharmaceutical Engineering – ChatGPT in regulated pharma* (2023) [9] [10] [12] [14]; OpenAI *FAQ risposta di ChatGPT* [13]

Checklist operativa finale (cosa fare e non fare)

- **Non inserire dati personali o segreti industriali** nei prompt di ChatGPT Enterprise, salvo stretta necessità. Anonimizza le informazioni sensibili ogni volta che è possibile.
- **Verifica le risposte importanti** di ChatGPT con fonti ufficiali o colleghi esperti prima di usarle in documenti o decisioni aziendali. Non dare mai per certo un output senza controlli esterni.
- Assicurati che la tua organizzazione abbia **firmato gli accordi necessari con OpenAI** (es. il DPA per il GDPR) prima di usare ChatGPT Enterprise su dati sensibili. Segui sempre le **policy interne** sull'uso di strumenti di AI e rispetto della privacy.
- **Usa solo l'account aziendale** per accedere a ChatGPT Enterprise (mai account personali). In questo modo tutte le conversazioni rimangono nell'ambiente controllato dall'azienda e soggetto alle misure di sicurezza aziendali.
- In caso di **dubbi** su cosa puoi o non puoi condividere con ChatGPT (es. dati di studi clinici, informazioni brevettuali), **contatta il reparto IT o legale** prima di procedere. È meglio chiedere chiarimenti che esporre dati in modo improprio.
- **Mantieni il controllo umano:** considera ChatGPT un assistente che ti fa risparmiare tempo, ma non un sostituto del tuo giudizio. Usa l'AI per la produttività, ma le decisioni finali e le revisioni critiche devono essere sempre effettuate da persone competenti.

---

[1] [2] [4] [6] [7] Enterprise privacy at OpenAI | OpenAI
https://openai.com/enterprise-privacy/

[3] [5] [8] ChatGPT for enterprise | OpenAI
https://openai.com/chatgpt/enterprise/

9 10 11 12 13 14 ChatGPT, BARD, and Other Large Language Models Meet Regulated Pharma | Pharmaceutical Engineering

https://ispe.org/pharmaceutical-engineering/july-august-2023/chatgpt-bard-and-other-large-language-models-meet