Privacy e Protezione dei Dati con ChatGPT versione Enterprise

Sicurezza e Crittografia dei Dati

Misure di Sicurezza Avanzate

OpenAI adotta misure di sicurezza avanzate per proteggere i dati forniti a ChatGPT Enterprise, garantendo la massima protezione delle informazioni sensibili.

Crittografia in Trasmissione

Ogni messaggio inviato o ricevuto viaggia in forma illeggibile a terzi grazie alla cifratura TLS, assicurando che i dati siano protetti durante il trasferimento.

Crittografia in Archiviazione

I contenuti vengono conservati in modo cifrato (AES-256) sui sistemi di OpenAI, proteggendo le informazioni anche quando sono archiviate sui server.

Controllo degli Accessi e Protezione

Chiave di Decrittazione

Anche intercettando il traffico o accedendo ai server, **nessuno possa leggere i dati** senza la chiave di decrittazione specifica.

Accesso Controllato

L'**accesso ai dati** è strettamente controllato all'interno dell'azienda per garantire massima sicurezza.

Utenti Autorizzati

Solo gli utenti autorizzati possono utilizzare ChatGPT Enterprise tramite le credenziali aziendali come il login Single Sign-On aziendale.

Gestione degli Accessi e Controllo del Personale

Gestione Amministratori IT

Gli amministratori IT possono gestire permessi e funzionalità disponibili per ciascun gruppo di utenti, mantenendo il controllo completo sull'accesso aziendale.

Personale Autorizzato OpenAI

Solo personale autorizzato può accedere ai dati delle conversazioni, garantendo massima protezione delle informazioni aziendali.

Accesso Eccezionale

L'accesso ai dati avviene solo in casi eccezionali: per risolvere incidenti tecnici, su richiesta esplicita dell'azienda, o per obblighi legali.

Queste misure assicurano che i contenuti scambiati con ChatGPT Enterprise non siano visibili né utilizzabili da persone non autorizzate.

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

Conformità GDPR e CCPA

ChatGPT Enterprise è allineato alle principali **normative sulla protezione dei dati** come il GDPR (Regolamento Generale sulla Protezione dei Dati per l'UE) e il CCPA (legge sulla privacy per la California).

Supporto alla Conformità Legale

L'uso di ChatGPT Enterprise può essere configurato per supportare la conformità legale, rispettando i diritti degli interessati e minimizzando la conservazione dei dati personali.

Certificazioni di Sicurezza

OpenAI ha ottenuto certificazioni di sicurezza indipendenti che attestano l'affidabilità dei controlli interni, incluso un audit **SOC 2 Type 2** superato con successo. Questa certificazione – rilasciata dopo verifica da parte di auditor terzi

In pratica questo conferma che OpenAI adotta standard industriali rigorosi in materia di sicurezza, riservatezza e integrità dei dati nelle sue piattaforme.

Data Resincy & Sovranità dei Dati

Opzioni di Data Residency

OpenAI fornisce opzioni di **data residency** (residenza dei dati) per aiutare le organizzazioni a rispettare vincoli locali e normativi specifici.

Controllo Geografico

I clienti ChatGPT Enterprise possono richiedere che i dati siano archiviati solo in **specifiche regioni geografiche** come nell'Unione Europea.

Sovranità dei Dati

Queste opzioni permettono di ottemperare ai requisiti di **sovranità dei dati locali** e rispettare le normative nazionali e regionali.

Data Residency & Sovranità dei Dati

Settore Farmaceutico

Particolarmente rilevante per le **aziende farmaceutiche multinazionali** che devono garantire che i dati dei pazienti o i dati clinici non escano da determinati territori.

Localizzazione UE

Una casa farmaceutica con sede in Europa può impostare la **localizzazione dei dati in UE** per tutte le conversazioni, assicurando che le informazioni non vengano archiviate su server fuori dall'Europa.

Dati Clinici Protetti

I dati di sperimentazioni cliniche europee rimangono **protetti territorialmente**, garantendo conformità alle normative locali sulla privacy sanitaria.

Esempio pratico: una casa farmaceutica europea adotta ChatGPT Enterprise per i propri dipendenti. Grazie alle funzionalità offerte, l'azienda verifica che OpenAI abbia le **certificazioni di sicurezza** adeguate (come SOC 2) e può quindi riferire agli auditor interni che il fornitore AI risponde agli standard di settore.

Supporto dedicato e garanzie contrattuali offerte da OpenAI

Accordi Contrattuali Specifici

OpenAI offre **accordi contrattuali specifici** ai clienti ChatGPT Enterprise per garantire ulteriore tranquillità nel trattamento e nella protezione dei dati aziendali.

Data Processing Addendum (DPA)

Le aziende possono sottoscrivere con OpenAI un **Data Processing Addendum (DPA)** – un **accordo sul trattamento dei dati** – che definisce in modo vincolante la gestione dei dati.

Conformità Normativa Garantita

Il DPA assicura che OpenAI gestirà i dati della tua organizzazione in conformità alle leggi sulla privacy, come il GDPR, offrendo protezione legale vincolante.

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.