Gestify – Informativa Connettore MCP per assistenti di IA

Ultimo aggiornamento: 25 settembre 2025

1. Oggetto e destinatari

La presente informativa descrive come funziona il Connettore MCP di Gestify, quali dati rende accessibili agli assistenti di intelligenza artificiale collegati dal Cliente e come si ripartiscono ruoli e responsabilità.

Si rivolge ai Clienti di Gestify (di seguito "Cliente") e agli utenti da questi autorizzati. È resa da **Tecnos S.r.l.**, con sede in Via Muller 35/17, Verbania (VB), P.IVA 02370320034 (di seguito "Tecnos"), che sviluppa ed eroga la piattaforma Gestify.

L'informativa integra, e non sostituisce, le Condizioni generali di Tecnos (Planet e Gestify), l'Accordo sul trattamento dei dati personali ai sensi dell'art. 28 GDPR ("DPA") e l'informativa privacy di Tecnos.

2. Cos'è il Connettore MCP e come funziona

Il Connettore MCP permette a un assistente di IA scelto dal Cliente di consultare, **in sola lettura**, i dati del Cliente in Gestify. Usa il Model Context Protocol (MCP), uno standard aperto compatibile con assistenti come Claude, ChatGPT e altri.

Il Connettore è disponibile solo se il relativo modulo è attivo sul piano dell'azienda e se l'utente ha ricevuto il permesso dedicato. Funziona così:

1. L'amministratore del Cliente assegna il permesso di accesso al Connettore agli utenti che devono usarlo.
2. L'utente avvia la connessione dalla propria app di IA e accede a Gestify con le proprie credenziali, tramite OAuth 2.1 con PKCE. All'assistente non viene mai consegnata la password.
3. In una schermata di consenso l'utente sceglie l'azienda, può escludere le aree di dati che non vuole concedere (ad es. anagrafiche, documenti, magazzino, margini e utili) e accetta le informative.
4. Ogni connessione vale per un solo utente e una sola azienda.
5. Quando l'utente pone una domanda, l'assistente chiama gli strumenti esposti da Gestify. Gestify restituisce solo i dati che quell'utente può già vedere, nei limiti delle aree concesse.
6. L'assistente elabora i dati sui sistemi del proprio fornitore e risponde all'utente.

Gestify non è un sistema di IA e non genera le risposte: queste sono prodotte dall'assistente scelto dal Cliente, che può commettere errori. Gestify non invia dati di propria iniziativa, ma risponde solo alle richieste che l'app di IA fa a nome dell'utente.

3. Ruoli nel trattamento dei dati personali

Il Cliente resta titolare dei dati che rende accessibili tramite il Connettore; Tecnos agisce come suo responsabile; il fornitore dell'assistente è un soggetto scelto dal Cliente, estraneo al rapporto con Tecnos.

Soggetto	Ruolo ai sensi del GDPR	Cosa fa
Cliente	Titolare del trattamento (art. 4, n. 7)	Decide se attivare il Connettore, quali utenti e quali dati abilitare, quale assistente usare e per quali finalità
Tecnos S.r.l.	Responsabile del trattamento (art. 28), secondo il DPA	Ospita i dati in Gestify ed esegue le richieste MCP autenticate per conto del Cliente
Fornitore dell'assistente di IA (es. Anthropic, OpenAI)	Soggetto terzo scelto dal Cliente; il ruolo (responsabile del Cliente o titolare autonomo) dipende dal contratto tra Cliente e fornitore	Riceve i dati restituiti da Gestify ed elabora le risposte

Il fornitore dell'assistente **non è un sub-responsabile di Tecnos**: Tecnos non lo seleziona, non ha un contratto con esso per questo servizio e non ne controlla il trattamento. La trasmissione dei dati verso l'assistente avviene su istruzione documentata del Cliente, data con l'attivazione del Connettore e con l'autorizzazione dell'utente.

4. Dati accessibili e perimetro delle autorizzazioni

L'assistente vede esattamente ciò che vede l'utente che lo ha collegato, e nulla di più: il Connettore applica gli stessi ruoli e permessi configurati in Gestify, ridotti delle aree escluse al momento del consenso.

Il Connettore espone 37 strumenti di consultazione, più uno strumento di contesto che indica all'assistente azienda e utente collegati. Le aree di dati accessibili sono:

Area	Esempi di dati
Anagrafiche	Clienti, fornitori e contatti: ragioni sociali, nomi, recapiti, indirizzi, codice fiscale, IBAN e coordinate bancarie; scadenze e statistiche
Documenti	Preventivi, ordini, DDT, fatture e loro righe; fatturato, scadenze, saldo ordini
Commesse e progetti	Totali e fatturato di commessa, contabilità di

Area	Esempi di dati
	progetto, offerte, SAL
Interventi e rapportini	Interventi previsti ed eseguiti, righe, economia, ore di manodopera
Magazzino e listini	Articoli, giacenze, movimenti, impegnato e ordinato, listini, prezzi speciali, articoli più venduti
Contabilità	Prima nota, saldi dei conti, saldo IVA, scadenzario
Margini e provvigioni	Margini delle offerte, provvigioni degli agenti

Alcune aree contengono dati personali di dipendenti e collaboratori del Cliente, ad esempio ore di manodopera nei rapportini e provvigioni degli agenti.

Il Connettore **non espone mai** credenziali e segreti: password, hash, token, chiavi API e codici di autenticazione a più fattori. Gestify non è progettato per trattare categorie particolari di dati (art. 9 GDPR) né dati giudiziari (art. 10): il Cliente non deve inserirli nei campi del gestionale.

Il Cliente controlla l'accesso così:

- **Per utente:** l'amministratore assegna o toglie il permesso di accesso al Connettore.
- **Per area di dati:** l'utente che non vede un modulo in Gestify non lo vede neanche tramite l'assistente; al consenso può inoltre escludere intere aree.
- **Per strumento:** non è previsto un pannello per abilitare o disabilitare i singoli strumenti.

5. Trasmissione al fornitore dell'assistente e trasferimenti fuori dall'UE

I dati restituiti da Gestify escono dall'infrastruttura di Tecnos e sono trattati secondo il contratto tra il Cliente e il fornitore dell'assistente. Da quel momento Tecnos non ne controlla conservazione, uso o cancellazione.

Molti fornitori di assistenti hanno sede o server fuori dallo Spazio economico europeo, in particolare negli Stati Uniti. Spetta al Cliente verificare che il trasferimento sia lecito ai sensi del Capo V GDPR, ad esempio tramite:

- adesione del fornitore all'EU-U.S. Data Privacy Framework;
- clausole contrattuali tipo della Commissione europea nel contratto con il fornitore;
- opzioni di trattamento o conservazione dei dati nell'UE, se offerte dal fornitore.

Il Cliente deve inoltre verificare, nel piano sottoscritto con il fornitore, se i dati possono essere usati per addestrare i modelli e per quanto tempo restano memorizzati (cronologia delle conversazioni, memoria, log). Tecnos raccomanda piani professionali o aziendali che escludano l'addestramento sui dati del Cliente.

6. Sola lettura e controllo umano

Il Connettore consente solo di leggere i dati: l'assistente non può creare, modificare o cancellare nulla in Gestify.

Il vincolo è doppio. Gli strumenti esposti sono esclusivamente di consultazione e, in aggiunta, il server rifiuta qualsiasi operazione di scrittura proveniente da una sessione aperta tramite il Connettore, anche se qualcuno tentasse di forzarla.

Le risposte dell'assistente possono comunque contenere errori di interpretazione o di calcolo: l'utente deve verificarle prima di usarle in documenti, comunicazioni o decisioni.

Il Connettore non deve essere usato per decisioni basate unicamente su un trattamento automatizzato che producano effetti giuridici o analogamente significativi su persone fisiche (art. 22 GDPR), ad esempio blocco di un cliente o valutazioni di affidabilità, senza intervento umano.

7. Misure di sicurezza e registrazione degli accessi

Tecnos protegge il Connettore con le misure tecniche e organizzative previste dal DPA per la piattaforma Gestify, oltre a quelle specifiche elencate qui. Server applicativi, database e log sono ospitati su Amazon Web Services (AWS), regione eu-central-1 (Francoforte, Germania).

- **Autenticazione:** solo OAuth 2.1 con PKCE (metodo S256 obbligatorio). Non esistono token personali generati in Gestify.
- **Durata delle credenziali:** il token di accesso dura 10 minuti; il token di rinnovo dura 180 giorni e cambia a ogni utilizzo. Se un token di rinnovo già usato viene ripresentato, tutti i token della connessione vengono revocati. Nel database si conserva solo l'impronta (hash) dei token, mai il token in chiaro.
- **Revoca:** ogni utente vede e revoca in qualsiasi momento le proprie connessioni. Se all'utente viene tolto il permesso, o all'azienda il modulo, la connessione si interrompe entro 10 minuti. Interrompere le connessioni dei propri utenti, ad esempio quando un dipendente lascia l'azienda, spetta al Cliente, che lo fa togliendo il permesso. Tecnos può disattivare il Connettore per tutti solo per esigenze di sicurezza o di servizio.
- **Cifratura:** comunicazioni solo su HTTPS, con TLS 1.2 o superiore.
- **Limiti d'uso:** 60 richieste al minuto per connessione e 120 al minuto per azienda; al massimo 50 righe per risposta; 45 secondi di tempo massimo per richiesta; limite alle richieste contemporanee.
- **Registro delle richieste:** per ogni richiesta Gestify registra data, azienda, utente, connessione, strumento, esito, tempi, numero di righe restituite e parametri di ricerca. Il contenuto delle risposte non viene mai registrato. Le domande che l'utente scrive all'assistente non arrivano a Gestify: restano presso il fornitore dell'IA. I parametri di ricerca possono contenere dati personali, ad esempio il nome di un cliente cercato.
- **Registro degli accessi:** autorizzazioni, rinnovi, revoche e consensi sono registrati con indirizzo IP e tipo di client (user agent).
- **Conservazione dei log:** i registri servono a sicurezza, assistenza tecnica, rendicontazione ed eventuale fatturazione del servizio, con tempi diversi per ciascun dato. I log tecnici del server e

degli accessi sono conservati 6 mesi e poi cancellati automaticamente. Il contenuto delle richieste, cioè i parametri e i filtri usati dall'assistente, è cancellato automaticamente dopo 6 mesi. I dati di utilizzo (utente, strumento, data e ora, esito) sono conservati per la durata del contratto e, dopo, per il periodo previsto dalla normativa civilistica e fiscale. I dati che Gestify restituisce all'assistente non sono conservati da Tecnos. I log sono consultabili solo da personale autorizzato di Tecnos, non dall'amministratore del Cliente.

- **Istruzioni malevole (prompt injection):** testi presenti nei dati, ad esempio note inserite da terzi, potrebbero indurre l'assistente a risposte fuorvianti o a passare i dati ad altri strumenti collegati all'app di IA. La sola lettura e i permessi limitano questo rischio, che non può essere escluso del tutto.

AWS opera come sub-responsabile di Tecnos ed è indicato nell'elenco dei sub-responsabili allegato al DPA. In caso di violazione dei dati personali che coinvolga il Connettore, Tecnos informa il Cliente senza ingiustificato ritardo, come previsto dal DPA e dall'art. 33 GDPR.

8. Inquadramento ai sensi del Regolamento (UE) 2024/1689 (AI Act)

Il Connettore MCP è un'interfaccia di accesso ai dati e non rientra nella definizione di sistema di IA: gli obblighi dell'AI Act ricadono sul fornitore dell'assistente e, come utilizzatore ("deployer"), sul Cliente.

Quadro aggiornato al 6 ottobre 2026, dopo il Regolamento (UE) 2026/1744 (Omnibus digitale sull'IA), in vigore dal 27 luglio 2026:

Obbligo AI Act	Su chi ricade	Applicazione
Informare le persone che interagiscono con un sistema di IA (art. 50, par. 1)	Fornitore dell'assistente	Dal 2 agosto 2026
Marcatura leggibile da macchina dei contenuti generati (art. 50, par. 2)	Fornitore dell'assistente	Dal 2 agosto 2026; fino al 2 dicembre 2026 per i sistemi già sul mercato prima del 2 agosto 2026
Alfabetizzazione in materia di IA del personale (art. 4)	Cliente, come deployer	In vigore; ridotto dall'Omnibus a obbligo di adoperarsi
Obblighi per sistemi ad alto rischio (Allegato III)	Fornitore e deployer	Rinviati al 2 dicembre 2027

L'uso di un assistente collegato a un gestionale per consultare documenti, magazzino o clienti non è, di norma, un uso ad alto rischio. Lo diventa se il Cliente lo impiega per finalità dell'Allegato III, ad esempio selezione o valutazione del personale o valutazione del merito creditizio di persone fisiche: in tal caso si applicano gli obblighi del deployer (art. 26).

In Italia, la Legge 23 settembre 2025, n. 132 prevede inoltre che il datore di lavoro informi i lavoratori sull'uso di sistemi di IA (art. 11). L'Assistente IA integrato in Gestify, fornito direttamente da Tecnos, è disciplinato da un'informativa separata.

9. Obblighi e raccomandazioni per il Cliente

Attivando il Connettore, il Cliente dichiara di aver valutato i punti seguenti e se ne assume la responsabilità come titolare del trattamento.

- ☐ Ha scelto il fornitore dell'assistente e verificato contratto, ruolo privacy, trasferimenti extra-UE e uso dei dati per l'addestramento.
- ☐ Ha aggiornato la propria informativa verso clienti, fornitori e dipendenti, indicando l'uso di assistenti di IA e i relativi destinatari (artt. 13-14 GDPR).
- ☐ Ha aggiornato il registro delle attività di trattamento (art. 30 GDPR) e valutato la necessità di una valutazione d'impatto (art. 35 GDPR).
- ☐ Ha assegnato il permesso di accesso al Connettore solo agli utenti che ne hanno bisogno e li ha invitati a escludere, al consenso, le aree di dati non necessarie; toglie il permesso quando un utente non deve più usare il Connettore, ad esempio alla cessazione del rapporto.
- ☐ Ha formato gli utenti sull'uso dell'assistente e sui suoi limiti (art. 4 AI Act) e informato i lavoratori (art. 11 L. 132/2025).
- ☐ Ha stabilito che le risposte dell'assistente vanno verificate prima di essere usate in documenti, comunicazioni o decisioni.
- ☐ Non usa il Connettore per finalità ad alto rischio dell'AI Act né per decisioni interamente automatizzate ai sensi dell'art. 22 GDPR.

10. Responsabilità, disattivazione e contatti

Tecnos risponde del corretto funzionamento del Connettore e del rispetto dei permessi configurati, non del contenuto delle risposte dell'assistente né del trattamento svolto dal suo fornitore.

- **Esclusioni:** Tecnos non risponde di errori, omissioni o azioni dell'assistente di IA, né dell'uso dei dati da parte del suo fornitore, nei limiti consentiti dalla legge e dalle Condizioni generali del servizio.
- **Disattivazione:** il Cliente può togliere il permesso a uno o più utenti, e le loro connessioni si interrompono entro 10 minuti. La gestione delle connessioni dei propri utenti spetta al Cliente. Ogni utente può inoltre revocare subito le proprie connessioni. I dati già trasmessi al fornitore dell'assistente vanno gestiti con quest'ultimo.
- **Diritti degli interessati:** le persone i cui dati sono in Gestify esercitano i propri diritti (artt. 15-22 GDPR) verso il Cliente, titolare del trattamento. Tecnos assiste il Cliente come previsto dal DPA.
- **Modifiche:** Tecnos aggiorna questa informativa in caso di nuove funzioni del Connettore o di modifiche normative, in particolare all'esito della revisione del GDPR prevista dall'Omnibus digitale.
- **Contatti:** Tecnos S.r.l., Via Muller 35/17, Verbania (VB) — privacy@tecnositalia.it — Responsabile della protezione dei dati (DPO): avv. Mattia Tacchini, mt@mattiatacchini.it, PEC mattia.tacchini@pec.it.

Riferimenti normativi

- Regolamento (UE) 2016/679 (GDPR), in particolare artt. 4, 12-14, 22, 28, 30, 32-35 e Capo V.

- Regolamento (UE) 2024/1689 (AI Act), artt. 4, 26 e 50, come modificato dal Regolamento (UE) 2026/1744.
- Legge 23 settembre 2025, n. 132 (disposizioni nazionali in materia di intelligenza artificiale).