OTTAVIO

Sicurezza e privacy dei dati

Come Ottavio tratta le informazioni della tua azienda



Ottavio è un collega IA che lavora dentro Slack, Teams, Discord o WhatsApp e si collega agli strumenti che la tua azienda usa già. Per fare bene il suo lavoro deve poter consultare informazioni aziendali. Questo documento spiega **cosa vede e cosa no, dove vengono conservati i dati, chi può accedervi e come mantieni il controllo** in ogni momento.

1. Il principio: i tuoi dati restano tuoi

- **Consulto, non copio.** Interrogo i tuoi strumenti quando mi serve qualcosa (un numero, un avviso) e conservo solo ciò che produco: il report del giorno, gli avvisi e le risposte. Non tengo copie del tuo CRM né del tuo database.
- **Sola lettura, accesso minimo.** Ogni collegamento ha permessi di sola lettura e copre solo ciò che serve al compito concordato.
- **Decidi tu, e puoi revocare.** Qualsiasi accesso si toglie con un clic dallo strumento stesso, senza dover passare da noi.

2. Come mi collego ai tuoi strumenti

- **Strumenti SaaS** (HubSpot, Salesforce, Notion, Asana, Google Workspace…): tramite OAuth, con permessi di sola lettura. Sei tu ad autorizzare e sei tu a revocare.
- **Database interni:** con un utente di sola lettura che vede soltanto alcune **viste** preparate dal tuo team, con i numeri e senza colonne sensibili (niente email, telefoni o documenti d'identità). Scegli tu cosa vedo.
- **Riunioni:** leggo le note e le trascrizioni delle riunioni che decidi di condividere con me.
- **Niente password in chat.** Le credenziali si autorizzano via OAuth o si configurano in modo sicuro, mai scritte in una conversazione.

3. Dati personali: il minimo indispensabile

- I dati personali dei tuoi clienti **non compaiono mai in un canale**. Se una persona autorizzata ne ha bisogno, li riceve in privato tramite un **link temporaneo** che scade e registra chi lo apre.
- Quando non serve identificare nessuno, lavoro con **dati aggregati** o **pseudonimizzati** prima di inviarli al modello di IA.
- Ognuno vede solo ciò che **il suo ruolo** gli consente.

4. Cosa conservo e per quanto tempo

- **Conservazione predefinita: 90 giorni.** Le conversazioni, i report e gli avvisi che produco vengono cancellati automaticamente dopo questo periodo. Puoi ridurlo a 30 giorni o fissare la durata che ti serve.
- **Configurazione:** ciò che mi hai insegnato (persone, avvisi, tono, regole) resta salvato per tutta la durata del servizio, così posso continuare a lavorare.
- **Alla fine del servizio** cancelliamo tutte le informazioni della tua azienda e ti consegniamo un **certificato di cancellazione**. Prima, se lo chiedi, te le esportiamo.

5. Chi può accedere alle tue informazioni

- **Credenziali cifrate** in un archivio separato, isolato per cliente.
- **Di norma nessuno del team di Ottavio legge i tuoi contenuti.** Se mai servisse per l'assistenza, succede solo con il tuo permesso esplicito e resta registrato.
- **Registro di audit:** resta traccia di cosa ho consultato, quando e per conto di chi. Puoi richiederlo quando vuoi.
- **Isolamento:** i dati di ogni cliente sono separati da quelli degli altri.

6. Dentro la tua chat

- **Una persona approva** ciò che conta prima che venga pubblicato (per esempio, il report del giorno).
- **Ogni numero viene verificato** sulla fonte prima di uscire. Se non torna, non esce.
- **Rispondo solo agli utenti autorizzati** della tua azienda e ignoro le istruzioni di terzi che cercano di manipolarmi.
- **Regole che non si possono disattivare:** niente dati personali nei canali, niente numeri inventati, niente consigli di investimento.

7. Il modello di intelligenza artificiale

- Lavoro con **Claude di Anthropic**, tramite la sua **API enterprise**. Per contratto, i dati inviati tramite l'API **non vengono usati per addestrare modelli**.
- Per le aziende che ne hanno bisogno, posso usare Claude **tramite Amazon Web Services in una regione europea** (AWS Bedrock): così il trattamento resta dentro l'infrastruttura AWS in Europa.

8. Tre modi per installarmi

Livello	Dove lavoro	Per chi
Cloud	Server di Ottavio nell'Unione Europea, con ogni cliente isolato.	Team che vogliono partire subito.
Dedicato	Un server riservato alla tua azienda, nell'Unione Europea.	Aziende con requisiti di sicurezza più stringenti.
Nel tuo cloud	Dentro la tua infrastruttura (AWS, Azure, Google Cloud…). I dati non escono mai di casa.	Settori regolamentati: finanza, sanità, pubblica amministrazione.

9. Conformità e contratti

- **GDPR.** La tua azienda è titolare del trattamento e Ottavio agisce come **responsabile del trattamento** (art. 28), con un **accordo sul trattamento dei dati (DPA)** firmato.
- **Elenco dei sub-responsabili** (hosting, fornitore del modello di IA) disponibile e aggiornato; ti avvisiamo prima di qualsiasi cambiamento.
- **Accordo di riservatezza (NDA)** su richiesta.
- **Incidenti:** se si verificasse un incidente di sicurezza che ti riguarda, ti avvisiamo **senza ritardo**, così puoi adempiere ai tuoi obblighi.

Altre domande? Scrivici a **hola@ottavio.bot** o chiedi direttamente a Ottavio su **ottavio.bot**.