OTTAVIO

Sicurezza e privacy dei dati



Come lavora Ottavio con le informazioni della tua azienda

Ottavio è un collega di squadra con IA che vive nel vostro Slack, Teams, Discord o WhatsApp e si collega ai vostri strumenti. Per lavorare bene deve vedere informazioni aziendali. Questo documento spiega **cosa vede, cosa non vede, dove si conserva, chi può accedervi e come mantenete il controllo** in ogni momento.

1. Il principio: i tuoi dati restano tuoi

- **Consulto, non copio.** Interrogo i vostri strumenti quando serve (una cifra, un avviso) e conservo solo ciò che genero: il report del giorno, gli avvisi e le risposte. Non tengo copie del vostro CRM né del vostro database.
- **Sola lettura e accesso minimo.** Ogni collegamento ha permessi di sola lettura e solo su ciò che serve al compito concordato.
- **Decidete voi e potete revocare.** Qualsiasi accesso si toglie con un clic dal vostro stesso strumento, senza dipendere da noi.

2. Come mi collego ai vostri strumenti

- **Strumenti SaaS** (HubSpot, Salesforce, Notion, Asana, Google Workspace…): tramite OAuth, con permessi di sola lettura. Autorizzate voi e revocate voi.
- **Database propri:** con un utente di sola lettura che vede soltanto alcune **viste** preparate dal vostro team, con cifre e senza colonne sensibili (niente email, telefoni o documenti d'identità). Scegliete voi cosa vedo.
- **Riunioni:** leggo le note e le trascrizioni delle riunioni che decidete 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 vostri clienti **non compaiono mai in un canale**. Se qualcuno autorizzato 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 **cifre aggregate** o con dati **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.** Conversazioni, report e avvisi che genero si cancellano automaticamente dopo questo periodo. Potete ridurlo a 30 giorni o fissare quello che vi serve.
- **Configurazione:** ciò che mi avete insegnato (persone, avvisi, tono, regole) resta finché dura il servizio, per poter continuare a lavorare.
- **Alla fine del servizio** cancelliamo tutte le vostre informazioni e vi consegniamo un **certificato di cancellazione**. Prima, se lo chiedete, ve le esportiamo.

5. Chi può accedere alle vostre informazioni

- **Credenziali cifrate** in un archivio separato, isolato per cliente.
- **Nessuno del team di Ottavio legge i vostri contenuti per impostazione predefinita.** Se mai servisse per l'assistenza, avviene solo con il vostro permesso esplicito e resta registrato.
- **Registro di audit:** resta traccia di cosa ho consultato, quando e per chi. Potete richiederlo quando volete.
- **Isolamento:** i dati di ogni cliente sono separati da quelli degli altri.

6. Dentro la vostra chat

- **Una persona approva** ciò che è importante prima di pubblicarlo (per esempio, il report del giorno).
- **Ogni cifra viene verificata** sulla sua fonte prima di uscire. Se non torna, non esce.
- **Rispondo solo a utenti autorizzati** della vostra azienda e ignoro le istruzioni di terzi che cercano di manipolarmi.
- **Regole che non si possono disattivare:** niente dati personali nei canali, niente cifre inventate, 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 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 in fretta.
Dedicato	Un server solo per la vostra azienda, nell'Unione Europea.	Aziende con esigenze di sicurezza più alte.
Nel vostro cloud	Dentro la vostra infrastruttura (AWS, Azure, Google Cloud…). I vostri dati non escono di casa.	Settori regolamentati: finanza, sanità, pubblica amministrazione.

9. Conformità e contratti

- **GDPR.** Voi siete titolari 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; vi avvisiamo prima di qualsiasi cambiamento.
- **Accordo di riservatezza (NDA)** su richiesta.
- **Incidenti:** se si verificasse un incidente di sicurezza che vi riguarda, vi avvisiamo **senza ritardo** perché possiate adempiere ai vostri obblighi.

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