OTTAVIO

Seguridad y privacidad de los datos



Cómo trabaja Ottavio con la información de tu empresa

Ottavio es un compañero de equipo con IA que vive en vuestro Slack, Teams, Discord o WhatsApp y se conecta a vuestras herramientas. Para hacerlo bien necesita ver información de la empresa. Este documento explica **qué ve, qué no ve, dónde se guarda, quién puede acceder y cómo mantenéis el control** en todo momento.

1. El principio: tus datos siguen siendo tuyos

- **Consulto, no copio.** Pregunto a vuestras herramientas cuando lo necesito (una cifra, un aviso) y solo guardo lo que genero: el parte del día, los avisos y las respuestas. No mantengo réplicas de vuestro CRM ni de vuestra base de datos.
- **Solo lectura y mínimo acceso.** Cada conexión tiene permisos de lectura y solo sobre lo necesario para la tarea acordada.
- **Vosotros decidís y podéis revocar.** Cualquier acceso se retira en un clic desde vuestra propia herramienta, sin depender de nosotros.

2. Cómo me conecto a vuestras herramientas

- **Herramientas SaaS** (HubSpot, Salesforce, Notion, Asana, Google Workspace…): por OAuth, con permisos de solo lectura. Vosotros autorizáis y vosotros revocáis.
- **Bases de datos propias:** con un usuario de solo lectura que únicamente ve unas **vistas** preparadas por vuestro equipo, con cifras y sin columnas sensibles (sin emails, teléfonos ni documentos de identidad). Vosotros elegís qué veo.
- **Reuniones:** leo las notas y transcripciones de las reuniones que vosotros decidís compartir conmigo.
- **Nada de contraseñas en el chat.** Las credenciales se autorizan por OAuth o se configuran de forma segura, nunca se escriben en una conversación.

3. Datos personales: los mínimos

- Los datos personales de vuestros clientes **nunca aparecen en un canal**. Si alguien con permiso los necesita, los recibe en privado mediante un **enlace temporal** que caduca y deja registro de quién lo abre.
- Cuando no hace falta identificar a nadie, trabajo con **cifras agregadas** o con datos **seudonimizados** antes de enviarlos al modelo de IA.
- Cada persona ve solo lo que **su rol** le permite.

4. Qué guardo y durante cuánto tiempo

- **Retención por defecto: 90 días.** Las conversaciones, partes y avisos que genero se borran automáticamente pasado ese plazo. Podéis reducirlo a 30 días o fijar el que necesitéis.
- **Configuración:** lo que me habéis enseñado (personas, avisos, tono, reglas) se conserva mientras dure el servicio, para poder seguir trabajando.
- **Al terminar el servicio** borramos toda vuestra información y os entregamos un **certificado de borrado**. Antes, si lo pedís, os la exportamos.

5. Quién puede acceder a vuestra información

- **Credenciales cifradas** en un almacén separado, aislado por cliente.
- **Nadie del equipo de Ottavio lee vuestro contenido por defecto.** Si alguna vez hace falta para soporte, se hace solo con vuestro permiso explícito y queda registrado.
- **Registro de auditoría:** queda constancia de qué consulté, cuándo y para quién. Podéis pedirlo cuando queráis.
- **Aislamiento:** los datos de cada cliente están separados de los de los demás.

6. Dentro de vuestro chat

- **Una persona aprueba** lo importante antes de publicarlo (por ejemplo, el parte del día).
- **Cada cifra se comprueba** contra su fuente antes de salir. Si no cuadra, no sale.
- **Solo atiendo a usuarios autorizados** de vuestra empresa e ignoro las instrucciones de terceros que intenten manipularme.
- **Reglas que no se pueden desactivar:** sin datos personales en canales, sin cifras inventadas, sin consejos de inversión.

7. El modelo de inteligencia artificial

- Trabajo con **Claude, de Anthropic**, a través de su **API empresarial**. Por contrato, los datos que se envían por la API **no se usan para entrenar modelos**.
- Para empresas que lo necesiten, puedo usar Claude **a través de Amazon Web Services en una región europea** (AWS Bedrock): así el tratamiento se queda dentro de la infraestructura de AWS en Europa.

8. Tres formas de instalarme

Nivel	Dónde funciono	Para quién
Cloud	Servidores de Ottavio en la Unión Europea, con cada cliente aislado.	Equipos que quieren empezar rápido.
Dedicado	Un servidor solo para vuestra empresa, en la Unión Europea.	Empresas con más exigencias de seguridad.
En vuestra nube	Dentro de vuestra propia infraestructura (AWS, Azure, Google Cloud…). Vuestros datos no salen de casa.	Sectores regulados: finanzas, salud, administración.

9. Cumplimiento y contratos

- **RGPD.** Vosotros sois responsables del tratamiento y Ottavio actúa como **encargado del tratamiento** (art. 28), con un **contrato de encargo (DPA)** firmado.
- **Lista de subencargados** (alojamiento, proveedor del modelo de IA) disponible y actualizada; os avisamos antes de cualquier cambio.
- **Acuerdo de confidencialidad (NDA)** a petición.
- **Incidentes:** si ocurriera cualquier incidente de seguridad que os afecte, os avisamos **sin demora** para que podáis cumplir vuestras obligaciones.

¿Más preguntas? Escríbenos a **hola@ottavio.bot** o pregúntale a Ottavio en **ottavio.bot**.