

Estándar de protección de datos y seguridad

Última actualización: 16 de octubre de 2026 · Versión 1.0

Este Estándar explica cómo BobOffice, LLC, operadora de ChatSales ("ChatSales", "nosotros"), protege los datos personales que nuestros clientes tratan en la plataforma ChatSales, las medidas de seguridad que aplicamos y las leyes de protección de datos que nuestras prácticas están diseñadas para respaldar. Aplica a todos los clientes de ChatSales.

Contenido

- | | |
|--------------------------------------|---|
| 1. Alcance | 9. Derechos de las personas |
| 2. Nuestro papel | 10. Transferencias internacionales |
| 3. Principios de protección de datos | 11. Conservación y eliminación |
| 4. Datos que tratamos | 12. Subencargados |
| 5. Estándar de seguridad | 13. Leyes y marcos que respalda este Estándar |
| 6. Quién ve qué dentro de su cuenta | 14. Responsabilidades del cliente |
| 7. Canales de mensajería e IA | 15. Contratos disponibles a solicitud |
| 8. Incidentes de seguridad | 16. Contacto |

1. Alcance

Este Estándar cubre los datos personales en las cuentas de clientes de ChatSales: contactos, conversaciones, embudos, difusiones, formularios y fuentes de conocimiento de la IA, así como los datos de los usuarios del cliente. Complementa nuestro [Aviso de privacidad](#) y los [Términos del servicio](#).

2. Nuestro papel

Respecto de los contactos y conversaciones de la cuenta de un cliente, **el cliente es el responsable** y ChatSales es el encargado (o service provider / data intermediary / operador, según la ley). Tratamos esos datos solo para prestar el servicio y según las instrucciones del cliente. **Nunca vendemos ni compartimos los datos de los clientes** para publicidad. ChatSales es responsable solo de sus propios datos de cuenta, facturación, seguridad y uso del producto.

3. Principios de protección de datos

Aplicamos los principios reconocidos internacionalmente: licitud y transparencia; limitación de la finalidad (solo para prestar el servicio); minimización; exactitud (el cliente puede editar y eliminar datos en cualquier momento); limitación del plazo de conservación (eliminación al terminar el servicio); integridad y confidencialidad (sección 5); y responsabilidad proactiva (medidas documentadas y este Estándar).

4. Datos que tratamos

Nombres, teléfonos, correos, nombres y fotos de perfil que entregan los canales de mensajería; contenido de mensajes (texto, imágenes, audio, video, documentos); etiquetas, notas, etapa del embudo, montos de venta y campos personalizados; respuestas de formularios; datos de referencia de anuncios (ID y título); y datos de cuenta y uso de los usuarios del cliente. El servicio no está diseñado para datos sensibles o de categorías especiales.

5. Estándar de seguridad

Cifrado: TLS 1.2 o superior en tránsito; AES-256 o equivalente en reposo.

Control de acceso: acceso por roles con mínimo privilegio, cuentas únicas, autenticación multifactor para acceso administrativo y revocación inmediata al cambiar funciones.

Red y aplicación: firewalls, segmentación de red, protección DDoS y límites de solicitudes; desarrollo seguro, parches de dependencias, análisis automatizados y evaluaciones periódicas de vulnerabilidades.

Resiliencia: respaldos, monitoreo y un proceso de respuesta a incidentes con funciones definidas.

Personas: obligaciones de confidencialidad para todo el personal con acceso a datos personales; políticas de seguridad revisadas al menos una vez al año.

5.1 Base de datos y alojamiento en Amazon Web Services (AWS)

Los datos de los clientes, incluida la base de datos y los mensajes y archivos almacenados, se alojan en **Amazon Web Services**. AWS opera sus centros de datos e infraestructura con las siguientes certificaciones y atestaciones auditadas de forma independiente (propias de AWS, publicadas en aws.amazon.com/compliance):

Certificación	Qué cubre
ISO/IEC 27001	Gestión de seguridad de la información
ISO/IEC 27017	Controles de seguridad en la nube
ISO/IEC 27018	Protección de datos personales en la nube
ISO/IEC 27701	Gestión de la información de privacidad
SOC 1, SOC 2 Type II, SOC 3	Auditorías independientes de controles de seguridad, disponibilidad y confidencialidad
PCI DSS Level 1	Seguridad de datos de tarjetas de pago
CSA STAR	Garantía de la Cloud Security Alliance

Bajo el modelo de responsabilidad compartida de AWS, AWS protege la infraestructura de la nube (centros de datos, hardware, red y virtualización) y la plataforma protege lo que corre sobre ella (accesos, configuración del cifrado, aplicación y datos). Los centros de datos de AWS cuentan con controles de acceso físico, vigilancia 24/7 y protecciones ambientales y de energía.

6. Quién ve qué dentro de su cuenta

Cada persona tiene su propio usuario. El cliente asigna roles (**Administrador, Editor, Agente**) y permisos uno por uno. Con "Acceso a todos los chats" apagado, un agente solo ve los chats asignados

a él o ella. El cliente también decide quién puede ver todos los contactos o exportarlos, para proteger su base si alguien deja el equipo.

7. Canales de mensajería e IA

Las conexiones de WhatsApp por API usan la **plataforma oficial WhatsApp Business de Meta**; las tarifas de mensajes las paga el cliente directamente a Meta. Las respuestas asistidas por IA funcionan solo donde el cliente las activa, con sus propias fuentes de conocimiento; los datos enviados a nuestro proveedor del modelo de IA por su API **no se usan para entrenar sus modelos**.

8. Incidentes de seguridad

Si un incidente de seguridad afecta los datos personales de un cliente, se lo notificamos **sin demora injustificada y dentro de 72 horas** desde que tengamos conocimiento, con la naturaleza del incidente, los datos y personas afectados, las consecuencias probables, las medidas tomadas y un punto de contacto, y apoyamos las notificaciones del cliente a autoridades y personas.

9. Derechos de las personas

El cliente puede ver, editar, exportar y eliminar contactos directamente en el producto, y lo asistimos con solicitudes de acceso, rectificación, cancelación o supresión, limitación, portabilidad, oposición y derechos equivalentes (incluidos los derechos ARCO en México). Las solicitudes que recibimos directamente se remiten al cliente.

10. Transferencias internacionales

Los datos pueden tratarse en los países de la sección 12. Cuando la ley exige un mecanismo de transferencia, usamos salvaguardas reconocidas: las Cláusulas Contractuales Tipo de la UE (2021/914), el Addendum de transferencias internacionales del Reino Unido y los mecanismos equivalentes de las demás leyes de la sección 13.

11. Conservación y eliminación

El cliente puede exportar sus datos en cualquier momento. Al terminar el servicio, o a solicitud, eliminamos sus datos personales **dentro de 30 días**, incluidas las copias en poder de subencargados, salvo que la ley obligue a conservarlos; los respaldos se sobrescriben en el curso ordinario.

12. Subencargados

Subencargado	Servicio	Lugar
TNT The Next Tech Ltd (ChatDaddy)	Tecnología y operación de la plataforma de mensajería	Hong Kong
Amazon Web Services, Inc.	Base de datos, alojamiento y almacenamiento de mensajes y archivos	Hong Kong (ap-east-1) + AWS regions
Google LLC (Google Cloud)	Servicios en la nube	Configurable regions / regiones configurables
Meta Platforms, Inc. / Meta Platforms Ireland Ltd	WhatsApp Business Platform, Instagram, Messenger	US, Ireland / global
OpenAI, L.L.C.	Modelo de IA para respuestas asistidas (solo si se activa)	US
Render Services, Inc.	Alojamiento del servicio de asistente de IA	US
Cloudflare, Inc.	Sitio web, seguridad perimetral, protección DDoS	Global
Stripe, Inc.	Procesamiento de pagos (solo facturación)	US

Avisamos a los clientes con 30 días de anticipación antes de agregar o sustituir un subencargado; el cliente puede oponerse por motivos razonables.

13. Leyes y marcos que respalda este Estándar

Región	Ley / marco	Cómo lo respaldamos
Unión Europea / EEE	General Data Protection Regulation (GDPR, EU 2016/679)	Términos de encargado (art. 28), Cláusulas Contractuales Tipo de la UE 2021/914 para transferencias
Reino Unido	UK GDPR and Data Protection Act 2018	Addendum de transferencias internacionales del Reino Unido
Suiza	Federal Act on Data Protection (FADP / nLPD)	CCT adaptadas para transferencias desde Suiza
Estados Unidos – California	California Consumer Privacy Act as amended by the CPRA (CCPA/CPRA)	Términos de service provider: sin venta ni compartición
Estados Unidos – otros estados	Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), Oregon (OCA) and other state privacy laws	Términos de encargado
Estados Unidos – federal	CAN–SPAM Act and TCPA (customer's messaging must have consent)	Consentimiento (opt-in) obligatorio para mensajes salientes
Canadá	Personal Information Protection and Electronic Documents Act (PIPEDA)	Responsabilidad y salvaguardas para proveedores de servicios
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)	Obligaciones de encargado, derechos ARCO
Brasil	Lei Geral de Proteção de Dados (LGPD)	Obligaciones de operador, cláusulas estándar de la ANPD para transferencias
Argentina	Ley 25.326 de Protección de los Datos Personales	Salvaguardas de encargado
Colombia	Ley 1581 de 2012 (Habeas Data)	Obligaciones de encargado
Chile	Ley 19.628 and Ley 21.719 (data protection reform)	Salvaguardas de encargado
Perú	Ley 29733 de Protección de Datos Personales	Obligaciones de encargado
Singapur	Personal Data Protection Act 2012 (PDPA)	Obligaciones de data intermediary, apoyo para notificación en 3 días
Malasia	Personal Data Protection Act 2010 (PDPA) and 2024 amendments	Obligaciones de encargado, apoyo para notificación de incidentes
Hong Kong	Personal Data (Privacy) Ordinance (PDPO, Cap. 486)	Salvaguardas de encargado

Filipinas	Data Privacy Act of 2012 (RA 10173)	Obligaciones de encargado de información personal
Indonesia	Personal Data Protection Law (UU PDP No. 27/2022)	Obligaciones de encargado
Tailandia	Personal Data Protection Act B.E. 2562 (PDPA)	Obligaciones de encargado
Japón	Act on the Protection of Personal Information (APPI)	Salvaguardas del encargado
Australia	Privacy Act 1988 and Australian Privacy Principles (APPs)	Salvaguardas transfronterizas (APP 8)
Emiratos Árabes Unidos	Federal Decree-Law No. 45 of 2021 (PDPL)	Obligaciones de encargado

ChatSales no cuenta con una certificación propia bajo estas leyes; nuestras prácticas y contratos están diseñados para respaldar el cumplimiento de nuestros clientes. Las certificaciones de AWS son propias de AWS.

14. Responsabilidades del cliente

El cliente es responsable de contar con una base legal y el consentimiento (opt-in) necesario para los contactos que carga y los mensajes que envía, de cumplir las políticas de WhatsApp y Meta, de configurar los permisos de sus usuarios y de su propio aviso de privacidad para sus clientes.

15. Contratos disponibles a solicitud

Cuando un cliente decide avanzar, firmamos: un **Contrato de encargo de tratamiento de datos (DPA)** (con las Cláusulas Contractuales Tipo de la UE y los términos por jurisdicción), un **Acuerdo mutuo de confidencialidad (NDA)** y una carta de confidencialidad a nombre de su empresa. También respondemos cuestionarios de seguridad. Solicítelos en info@chatsales.app.

16. Contacto

BobOffice, LLC (ChatSales) · privacidad y seguridad: info@chatsales.app · WhatsApp +1 302 314 2292 · trust.chatsales.app

Este Estándar describe nuestras prácticas y puede actualizarse; la versión vigente se publica en trust.chatsales.app. Cuando exista un contrato firmado con un cliente, ese contrato prevalece.