

Data Protection & Security Standard

Last updated: 16 October 2026 · Version 1.0

This Standard explains how BobOffice, LLC, operator of ChatSales ("ChatSales", "we"), protects the personal data that our customers process through the ChatSales platform, the security measures we apply, and the data protection laws our practices are designed to support. It applies to all ChatSales customers.

Contents

- | | |
|--------------------------------------|--|
| 1. Scope | 9. Rights of individuals |
| 2. Our role | 10. International transfers |
| 3. Data protection principles | 11. Retention and deletion |
| 4. Data we process | 12. Sub-processors |
| 5. Security standard | 13. Laws and frameworks this Standard supports |
| 6. Who sees what inside your account | 14. Customer responsibilities |
| 7. Messaging channels and AI | 15. Contracts available on request |
| 8. Security incidents | 16. Contact |

1. Scope

This Standard covers personal data in customer accounts on ChatSales: contacts, conversations, funnels, broadcasts, forms and AI knowledge sources, together with the data of customer users. It complements our [Privacy Notice](#) and [Terms of Service](#).

2. Our role

For the contacts and conversations in a customer's account, **the customer is the controller** and ChatSales is the processor (or service provider / data intermediary / encargado / operador, depending on the law). We process that data only to provide the service and on the customer's instructions. **We never sell or share customer data** for advertising. ChatSales is the controller only for its own account, billing, security and product-usage data.

3. Data protection principles

We apply the internationally recognised principles: lawfulness and transparency; purpose limitation (only to provide the service); data minimisation; accuracy (customers can edit and delete data at any time); storage limitation (deletion when the service ends); integrity and confidentiality (Section 5); and accountability (documented measures and this Standard).

4. Data we process

Names, phone numbers, email addresses, profile names and pictures provided by messaging channels; message content (text, images, audio, video, documents); tags, notes, funnel stage, deal values and

custom fields; form responses; advertising referral data (ad ID and title); and account and usage data of customer users. The service is not designed for special-category or sensitive data.

5. Security standard

Encryption: TLS 1.2 or higher in transit; AES-256 or equivalent at rest.

Access control: role-based access with least privilege, unique accounts, multi-factor authentication for administrative access, prompt revocation on role change.

Network and application: firewalls, network segmentation, DDoS protection and rate limiting; secure development, dependency patching, automated scanning and periodic vulnerability assessments.

Resilience: backups, monitoring and an incident response process with defined roles.

People: confidentiality obligations for all personnel with access to personal data; security policies reviewed at least annually.

5.1 Database and hosting on Amazon Web Services (AWS)

Customer data, including the database and stored messages and media, is hosted on **Amazon Web Services**. AWS operates its data centres and infrastructure under the following independently audited certifications and attestations (AWS's own, published at aws.amazon.com/compliance):

Certification	What it covers
ISO/IEC 27001	Information security management
ISO/IEC 27017	Cloud security controls
ISO/IEC 27018	Protection of personal data in the cloud
ISO/IEC 27701	Privacy information management
SOC 1, SOC 2 Type II, SOC 3	Independent audits of security, availability and confidentiality controls
PCI DSS Level 1	Payment card data security
CSA STAR	Cloud Security Alliance assurance

Under AWS's shared responsibility model, AWS secures the cloud infrastructure (data centres, hardware, network and virtualisation), and the platform secures what runs on it (access, encryption configuration, application and data). AWS data centres include physical access controls, 24/7 surveillance, and environmental and power protections.

6. Who sees what inside your account

Each person has their own user. Customers assign roles (**Admin, Editor, Agent**) and individual permissions. With "Access to all chats" turned off, an agent only sees the chats assigned to them. Customers also control who can see all contacts or export them, so their database stays protected if someone leaves the team.

7. Messaging channels and AI

WhatsApp API connections use **Meta's official WhatsApp Business Platform**; Meta's message fees are paid by the customer directly to Meta. AI-assisted replies run only where the customer enables them,

using the customer's own knowledge sources; data sent to our AI model provider through its API is **not used to train its models**.

8. Security incidents

If a security incident affects a customer's personal data, we notify the customer **without undue delay and within 72 hours** of becoming aware, with the nature of the incident, data and people affected, likely consequences, measures taken and a contact point, and we support the customer's own notifications to authorities and individuals.

9. Rights of individuals

Customers can view, edit, export and delete contacts directly in the product, and we assist with requests for access, rectification, erasure, restriction, portability, objection and equivalent rights (including ARCO rights in Mexico). Requests we receive directly are forwarded to the customer.

10. International transfers

Data may be processed in the countries listed in Section 12. Where the law requires a transfer mechanism, we use recognised safeguards: the EU Standard Contractual Clauses (2021/914), the UK International Data Transfer Addendum, and the equivalent mechanisms of the other laws in Section 13.

11. Retention and deletion

Customers can export their data at any time. When the service ends, or on request, we delete the customer's personal data **within 30 days**, including copies held by sub-processors, except where the law requires us to keep it; backups are overwritten in the ordinary course.

12. Sub-processors

Sub-processor	Service	Location
TNT The Next Tech Ltd (ChatDaddy)	Messaging platform technology and operations	Hong Kong
Amazon Web Services, Inc.	Database, hosting and storage of messages and media	Hong Kong (ap-east-1) + AWS regions
Google LLC (Google Cloud)	Cloud services	Configurable regions / regiones configurables
Meta Platforms, Inc. / Meta Platforms Ireland Ltd	WhatsApp Business Platform, Instagram, Messenger	US, Ireland / global
OpenAI, L.L.C.	AI model for AI-assisted replies (only when enabled)	US
Render Services, Inc.	Hosting of the AI assistant service	US
Cloudflare, Inc.	Website, edge security, DDoS protection	Global
Stripe, Inc.	Payment processing (billing data only)	US

We give customers 30 days' notice before adding or replacing a sub-processor; customers may object on reasonable grounds.

13. Laws and frameworks this Standard supports

Region	Law / framework	How we support it
European Union / EEA	General Data Protection Regulation (GDPR, EU 2016/679)	Processor terms (Art. 28), EU Standard Contractual Clauses 2021/914 for transfers
United Kingdom	UK GDPR and Data Protection Act 2018	UK International Data Transfer Addendum
Switzerland	Federal Act on Data Protection (FADP / nLPD)	SCCs adapted for Swiss transfers
United States – California	California Consumer Privacy Act as amended by the CPRA (CCPA/CPRA)	Service-provider terms: no selling or sharing
United States – other states	Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), Oregon (OCPA) and other state privacy laws	Processor terms
United States – federal	CAN-SPAM Act and TCPA (customer's messaging must have consent)	Opt-in and consent required for outbound messages
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	Accountability and safeguards for service providers
Mexico	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)	Encargado obligations, ARCO rights
Brazil	Lei Geral de Proteção de Dados (LGPD)	Operador obligations, ANPD standard clauses for transfers
Argentina	Ley 25.326 de Protección de los Datos Personales	Processor safeguards
Colombia	Ley 1581 de 2012 (Habeas Data)	Encargado obligations
Chile	Ley 19.628 and Ley 21.719 (data protection reform)	Processor safeguards
Peru	Ley 29733 de Protección de Datos Personales	Encargado obligations
Singapore	Personal Data Protection Act 2012 (PDPA)	Data intermediary obligations, 3-day notification support
Malaysia	Personal Data Protection Act 2010 (PDPA) and 2024 amendments	Data processor obligations, breach notification support
Hong Kong	Personal Data (Privacy) Ordinance (PDPO, Cap. 486)	Data processor safeguards
Philippines	Data Privacy Act of 2012 (RA 10173)	Personal information processor obligations

Indonesia	Personal Data Protection Law (UU PDP No. 27/2022)	Processor obligations
Thailand	Personal Data Protection Act B.E. 2562 (PDPA)	Data processor obligations
Japan	Act on the Protection of Personal Information (APPI)	Entrustee safeguards
Australia	Privacy Act 1988 and Australian Privacy Principles (APPs)	APP 8 cross-border safeguards
United Arab Emirates	Federal Decree–Law No. 45 of 2021 (PDPL)	Processor obligations

ChatSales does not hold its own certification under these laws; our practices and contracts are designed to support customers' compliance with them. AWS certifications are AWS's own.

14. Customer responsibilities

Customers are responsible for having a lawful basis and any required consent (opt-in) for the contacts they upload and the messages they send, for following WhatsApp and Meta policies, for configuring user permissions, and for their own privacy notice to their customers.

15. Contracts available on request

When a customer decides to proceed, we sign: a **Data Processing Agreement** (with the EU Standard Contractual Clauses and the jurisdiction-specific terms above), a **Mutual Non-Disclosure Agreement**, and a confidentiality letter addressed to the customer's company. We also complete security questionnaires. Request them at info@chatsales.app.

16. Contact

BobOffice, LLC (ChatSales) · privacy and security: info@chatsales.app · WhatsApp +1 302 314 2292 · trust.chatsales.app

This Standard describes our practices and may be updated; the current version is published at trust.chatsales.app. Where a signed agreement exists with a customer, that agreement prevails.