

Data Processing and Security Addendum (DPSA)

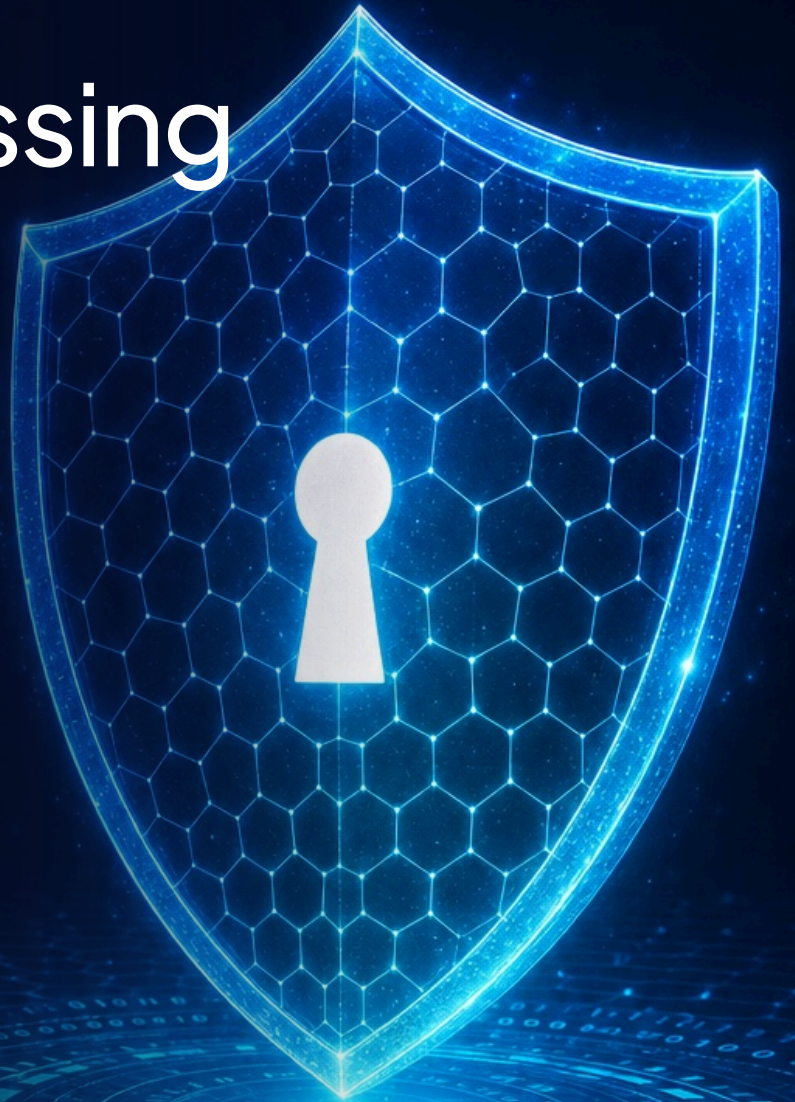


Table of Contents

	Definitions	
CHAPTER 1	Authorisation to Process Customer Personal Data	1.1
CHAPTER 2	Controller and Processor	2.1
CHAPTER 3	Customer Instructions	3.1
CHAPTER 4	Return or Deletion of Customer Personal Data	4.1
CHAPTER 5	Data Incident Notification	5.1
CHAPTER 6	Confidentiality Obligations of ChatSales Personnel	6.1
CHAPTER 7	Data Security	7.1
CHAPTER 8	Data Subject Rights	8.1
CHAPTER 9	Appointment of Sub-Processors	9.1
CHAPTER 10	Customer's Representations, Warranties and Undertakings	10.1
CHAPTER 11	Transfers of Customer Personal Data	11.1
CHAPTER 12	Jurisdiction-specific Requirements	12.1
CHAPTER 13	Governing Law and Order of Precedence	13.1
ANNEX 1	Technical and Organisational Security Measures	
ANNEX 2	Sub-Processors	

Data Processing and Security Addendum (DPSA)

This Data Processing and Security Addendum ("DPSA") supplements the ChatSales Terms of Service (available at trust.chatsales.app/legal/terms) or any other agreement between the Customer and BobOffice, LLC, operator of ChatSales ("ChatSales"), governing the Customer's use of the Services. This DPSA governs the Processing of Customer Personal Data. Administrative Information is Processed under the ChatSales Privacy Policy, and this DPSA does not apply to it.

This DPSA, including its annexes, is accepted by the Customer and takes effect on the date the Customer accepts the Terms of Service. If there is any conflict between the Terms of Service and this DPSA, this DPSA prevails. This DPSA continues in force until the Terms of Service end and, after that, for as long as ChatSales Processes Customer Personal Data.

Definitions

Unless stated otherwise, the following terms have the meanings below. Capitalised terms not defined here have the meaning given in the Terms of Service.

"Administrative Information": personal information the Customer provides to ChatSales to set up and manage its account, and personal information generated in connection with the Customer's use of the Services (for example, user logins and billing contacts).

"ChatSales Privacy Policy": the policy at trust.chatsales.app/legal/privacy, as updated from time to time.

"ChatSales Security Policy": the technical and organisational measures described in Annex 1, as updated by ChatSales from time to time without reducing the overall level of protection.

"Customer": the entity or person that has accepted the Terms of Service.

"Customer Data": any data, including personal information, that the Customer submits, uploads, transmits or displays using the Services, including contacts, conversations, funnels, broadcasts, forms and AI knowledge sources.

"Customer Personal Data": the personal data contained in the Customer Data. "Personal data" means any information relating to an identified or identifiable natural person, including "personal information" as defined in the Data Protection Laws.

"Controller": a person who, alone or jointly with others, determines the purposes and means of the Processing of Customer Personal Data.

"Data Incident": a breach of ChatSales' security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data Processed by ChatSales.

"Data Protection Laws": all data protection and privacy laws applicable to the Processing of Customer Personal Data, including the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA") and other US state privacy laws, Mexico's Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPDPPP"), Brazil's Lei Geral de Proteção de Dados ("LGPD"), Singapore's Personal Data Protection Act 2012, Malaysia's Personal Data Protection Act 2010, and Hong Kong's Personal Data (Privacy) Ordinance (Cap. 486).

"Data Subject": the individual to whom Customer Personal Data relates, including a "consumer" under the CCPA and a "titular" under the LFPDPPP and LGPD.

"Processing": any operation performed on Customer Personal Data, including collection, recording, storage, use, disclosure, transfer, erasure or destruction, or as otherwise defined in the Data Protection Laws.

"Processor": a person who Processes Customer Personal Data on behalf of a Controller.

"Services": the ChatSales services described in the Terms of Service.

"Standard Contractual Clauses": the standard contractual clauses for international transfers adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and, for the United Kingdom, the International Data Transfer Addendum issued by the Information Commissioner.

"Sub-Processor": any third party appointed by ChatSales to Process Customer Personal Data on its behalf under Clause 9.

"Supervisory Authority": a regulatory authority with jurisdiction over a Data Protection Law.

"Third Country": a country outside the European Economic Area that is not covered by an adequacy decision of the European Commission.

CHAPTER 1**Authorisation to Process Customer Personal Data**

- 1.1** In performing its obligations under the Terms of Service, ChatSales may Process Customer Personal Data in connection with the Customer's storage of, access to and Processing of Customer Data as part of the Services. This DPSA sets out each party's obligations for that Processing.
- 1.2** Each party will comply with all Data Protection Laws applicable to it in relation to Customer Personal Data.

CHAPTER 2**Controller and Processor**

- 2.1** The Customer is the Controller (or, where it acts for its own customers, a Processor) and ChatSales is the Processor (or Sub-Processor) in respect of Customer Personal Data.
- 2.2** ChatSales is an independent controller only for Administrative Information and for data it needs to secure, bill and improve the Services, which it handles under the ChatSales Privacy Policy. ChatSales does not sell Customer Personal Data or share it for advertising.

CHAPTER 3**Customer Instructions**

- 3.1** This DPSA and the Terms of Service, together with the Customer's configuration and use of the Services (including settings, automations, AI configuration and APIs), are the Customer's documented instructions for ChatSales' Processing of Customer Personal Data ("Documented Instructions").
- 3.2** ChatSales will Process Customer Personal Data only for the purposes of the Terms of Service and in line with the Documented Instructions, and will promptly tell the Customer if it cannot comply. Instructions outside the Documented Instructions require prior written agreement.
- 3.3** ChatSales will tell the Customer if, in its opinion, an instruction infringes the Data Protection Laws.

CHAPTER 4**Return or Deletion of Customer Personal Data**

- 4.1** During the subscription term, the Customer can retrieve, export and delete Customer Personal Data through the Services, and ChatSales will delete Customer Personal Data on the Customer's written request, unless the law prohibits it.

- 4.2** For 30 days after the subscription or the Terms of Service end, the Customer may export any remaining Customer Personal Data. After that period, ChatSales will delete Customer Personal Data within a further 30 days, including copies held by Sub-Processors, except where retention is required by law. Backups are overwritten in the ordinary course and remain protected by this DPSA until then. ChatSales will confirm deletion in writing on request.

CHAPTER 5

Data Incident Notification

- 5.1** ChatSales will notify the Customer without undue delay, and in any event within 72 hours, after becoming aware of a Data Incident, and will promptly take reasonable steps to minimise harm and secure the Customer Personal Data.
- 5.2** To help the Customer meet its own notification duties, ChatSales will describe, as far as it reasonably can, the nature of the Data Incident, the categories and approximate number of Data Subjects and records affected, its likely consequences, the measures taken or proposed, and a contact point, and will provide updates as more information becomes available.
- 5.3** An unsuccessful Data Incident is not subject to this Clause 5. An unsuccessful Data Incident is one that results in no unauthorised access to Customer Personal Data or to the equipment or facilities storing it, such as pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-in attempts, denial-of-service attacks, or packet sniffing that does not go beyond headers.
- 5.4** ChatSales is not required to assess Customer Personal Data to identify information subject to specific legal requirements, and its notification of or response to a Data Incident is not an acknowledgement of fault or liability.
- 5.5** The Customer is responsible for its use of the Services and for copies of Customer Personal Data it stores outside the Services, including: (a) using the Services' security features, such as user roles and permissions, appropriately for the risk; (b) securing the account credentials, systems and devices it uses to access the Services; and (c) backing up its Customer Personal Data as appropriate.
- 5.6** The parties will cooperate in good faith on any notification to Supervisory Authorities or Data Subjects relating to a Data Incident, and will consult each other before making public statements about it, without delaying any notification the law requires.

CHAPTER 6

Confidentiality Obligations of ChatSales Personnel

- 6.1** ChatSales will ensure that Customer Personal Data is accessible only to its duly authorised personnel and, subject to Clause 9, to its Sub-Processors and their duly authorised

personnel who need access to perform ChatSales' obligations under the Terms of Service.

- 6.2** ChatSales will ensure that everyone authorised to Process Customer Personal Data is bound by confidentiality, and that the obligations of this DPSA and the Customer's instructions are followed.

CHAPTER 7

Data Security

- 7.1** ChatSales implements and maintains appropriate technical and organisational measures against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Data, as described in Annex 1, including: (i) encryption of Customer Personal Data in transit and at rest; (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore availability of and access to Customer Personal Data in a timely manner after a physical or technical incident; and (iv) regularly testing, assessing and evaluating the effectiveness of these measures.
- 7.2** Customer data, including the database and stored messages and media, is hosted on Amazon Web Services (AWS), whose data centres and infrastructure are independently certified as described in Annex 1.

CHAPTER 8

Data Subject Rights

- 8.1** If ChatSales receives a request from a Data Subject relating to Customer Personal Data that identifies the Customer, ChatSales will advise the Data Subject to submit the request to the Customer and will forward it to the Customer. The Customer is responsible for responding, using the Services' functionality where appropriate (for example, to view, edit, export or delete contacts).
- 8.2** Taking into account the nature of the Processing, ChatSales will assist the Customer with appropriate technical and organisational measures, so far as practicable, to respond to requests to exercise Data Subject rights, including access, rectification, erasure, restriction, portability and objection, the ARCO rights under the LFPDPPP, and the rights under the CCPA and LGPD.

CHAPTER 9

Appointment of Sub-Processors

- 9.1** The Customer grants ChatSales general written authorisation to engage Sub-Processors to Process Customer Personal Data. ChatSales will enter into a written agreement with each

Sub-Processor containing data protection terms substantially the same as, and no less protective than, this DPSA. The current Sub-Processors are listed in Annex 2.

- 9.2** ChatSales will notify the Customer by email at least 30 days before adding or replacing a Sub-Processor. The Customer may object on reasonable data protection grounds within 14 days of the notice. If no objection is received, the change is deemed accepted. If the parties cannot resolve an objection in good faith, the Customer may terminate the affected Services and receive a pro-rata refund of prepaid fees for them.
- 9.3** ChatSales remains fully liable to the Customer for the performance of each Sub-Processor's data protection obligations.

CHAPTER 10

Customer's Representations, Warranties and Undertakings

- 10.1** The Customer represents and undertakes that throughout the term: (a) Customer Personal Data has been and will be collected in accordance with the Data Protection Laws, including any required consent or opt-in for the messages it sends; (b) its instructions to ChatSales comply with the Data Protection Laws; (c) the transfer of Customer Personal Data to ChatSales and its Processing under this DPSA is permitted by the Data Protection Laws; and (d) it has assessed that the Services are suitable for its purposes and that ChatSales' measures in Annex 1 provide an appropriate level of security.
- 10.2** The Customer will indemnify ChatSales against claims, losses and costs arising from a breach of this Clause 10, subject to the limitations in the Terms of Service.
- 10.3** If ChatSales faces an actual or potential claim relating to Customer Personal Data Processed under this DPSA, the Customer will promptly provide the information reasonably requested that is relevant to the defence of the claim.

CHAPTER 11

Transfers of Customer Personal Data

- 11.1** ChatSales may store and Process Customer Personal Data in the countries where it or its Sub-Processors maintain facilities, as listed in Annex 2, subject to Clause 11.2 and Clause 12.
- 11.2** Where the Processing involves a transfer of Customer Personal Data subject to the GDPR, UK GDPR or Swiss law to a Third Country, the Standard Contractual Clauses apply as set out in Clause 12A, unless another recognised transfer mechanism applies. Transfers under other Data Protection Laws are made with the safeguards those laws require.

CHAPTER 12

Jurisdiction-specific Requirements

- 12.1 A. Europe, United Kingdom and Switzerland.** (a) ChatSales will not Process EU Customer Personal Data in a Third Country except in compliance with the data importer's obligations in the Standard Contractual Clauses: Module 2 (controller to processor) where the Customer is a Controller, and Module 3 (processor to processor) where the Customer is a Processor. (b) For the Standard Contractual Clauses: Clause 7 (docking) applies; Clause 9(a) Option 2 (general authorisation, with the notice period in Clause 9.2 of this DPSA) applies; the optional wording in Clause 11 does not apply; the competent supervisory authority is that of the Customer's EU establishment or representative, or otherwise the Irish Data Protection Commission; and Clauses 17 and 18 are governed by the laws and courts of Ireland. (c) The Customer is the data exporter and ChatSales the data importer, and Annexes 1 and 2 complete the annexes of the Standard Contractual Clauses. (d) For the United Kingdom, the International Data Transfer Addendum applies; for Switzerland, references to the GDPR are read as references to the Swiss Federal Act on Data Protection. (e) If there is a conflict, the Standard Contractual Clauses prevail for EU Customer Personal Data.
- 12.2 B. United States.** (a) For the purposes of the CCPA, ChatSales acts as a "service provider", and under other US state privacy laws as a "processor". (b) ChatSales will not: sell or share Customer Personal Data (including for cross-context behavioural advertising); retain, use or disclose it for any purpose other than performing the Services, including any other commercial purpose; retain, use or disclose it outside the direct business relationship with the Customer; or combine it with personal information from other sources, except as the law permits. (c) ChatSales will notify the Customer if it can no longer meet these obligations. Terms such as "sell", "share", "business purpose" and "service provider" have the meanings given in the CCPA.
- 12.3 C. Mexico.** (a) Under the LFPDPPP, the Customer is the "responsable" and ChatSales the "encargado". (b) ChatSales will Process Customer Personal Data only on the Customer's instructions and for the purposes in the Customer's privacy notice, keep it confidential, apply the security measures in Annex 1, assist with ARCO requests, and delete it at the end of the relationship under Clause 4.
- 12.4 D. Brazil.** Under the LGPD, the Customer is the "controlador" and ChatSales the "operador". ChatSales will assist the Customer with Data Subject requests and notices to the ANPD, and international transfers will rely on a mechanism recognised by the LGPD, including the ANPD standard contractual clauses where required.
- 12.5 E. Singapore and Malaysia.** ChatSales acts as a data intermediary under Singapore's PDPA and as a data processor under Malaysia's PDPA. It will protect Customer Personal Data with reasonable security arrangements, stop retaining it when no longer needed for the Services, and notify Data Incidents under Clause 5 so the Customer can meet its own notification duties.

CHAPTER 13**Governing Law and Order of Precedence**

- 13.1** This DPSA is governed by the laws of the State of Delaware, United States, except where the Standard Contractual Clauses or a Data Protection Law require a different governing law for the matters they cover.
- 13.2** If there is a conflict, the following prevail in this order: (1) the Standard Contractual Clauses or other transfer mechanism, where applicable; (2) Clause 12; (3) the rest of this DPSA; (4) the Terms of Service.

ANNEX 1

Technical and Organisational Security Measures

ChatSales maintains a privacy and security programme to protect Customer Data, which includes the following measures.

Measure	Description
Data security	Encryption of data in transit with TLS 1.2 or higher and at rest with AES-256 or equivalent; data classification; authentication and access controls at the network, system and application levels.
Access control	Role-based access with least privilege; unique accounts with no shared credentials; multi-factor authentication for administrative access; prompt revocation when roles change. Inside the product, the Customer controls per-user roles (Admin, Editor, Agent) and permissions, including whether an agent can see all chats or contacts, or export data.
Network security	Isolation of production, development and office networks; firewalls and network segmentation; DDoS protection and rate limiting at the edge.
Application security	Secure development practices, dependency patching, automated security scanning and periodic vulnerability assessments.
Hosting on AWS	The database and stored messages and media are hosted on Amazon Web Services. AWS holds independently audited certifications and attestations including ISO/IEC 27001, 27017, 27018 and 27701, SOC 1, SOC 2 Type II and SOC 3, PCI DSS Level 1 and CSA STAR (published at aws.amazon.com/compliance). Under AWS' shared responsibility model, AWS secures the infrastructure and ChatSales secures what runs on it.
Physical and environmental security	AWS data centres apply strict physical access controls, 24/7 surveillance, and environmental and power protections.
Messaging channels and AI	WhatsApp connections use Meta's official WhatsApp Business Platform; Instagram and Messenger use Meta's official APIs. AI-assisted replies run only where the Customer enables them, and data sent to the AI model provider through its API is not used to train its models.
Incident management	Active service monitoring with a defined incident response process, enabling prompt detection, handling and notification of security incidents (Clause 5).
People	Confidentiality obligations for all personnel with access to Customer Personal Data; security policies reviewed at least annually.

ANNEX 2

Sub-Processors

Current Sub-Processors as of September 2026. Changes are notified under Clause 9.2.

Sub-Processor	Purpose	Location
Amazon Web Services, Inc.	Database, hosting and storage of messages and media	United States, Hong Kong and other AWS regions
Google LLC (Google Cloud)	Cloud services	Configurable regions
Meta Platforms, Inc. / Meta Platforms Ireland Ltd	WhatsApp Business Platform, Instagram and Messenger messaging	United States, Ireland / global
OpenAI, L.L.C.	AI model for AI-assisted replies (only when enabled)	United States
Render Services, Inc.	Hosting of the AI assistant service	United States
Cloudflare, Inc.	Website, edge security and DDoS protection	Global edge network
Stripe, Inc.	Payment processing (billing data only)	United States



Contact us for further inquiries

BobOffice, LLC (ChatSales)

info@chatsales.app

WhatsApp +1 302 314 2292

trust.chatsales.app