Data Processing Addendum

Zipchat Inc. | Version 2026-11 | Last updated: 12 November 2026

This Data Processing Addendum ("**DPA**") forms part of the Zipchat Terms of Service published at https://www.zipchat.ai/legal/terms-conditions (the "**Agreement**") between Zipchat Inc. ("**Zipchat**") and the customer that has accepted the Agreement ("**Customer**", and together with Zipchat, the "**Parties**").

This DPA is published at https://www.zipchat.ai/legal/dpa and applies automatically to Zipchat's processing of Personal Data on Customer's behalf from the date Customer accepts the Agreement. No signature is required. A Customer that needs a countersigned copy can request one at support@zipchat.ai. Zipchat enters into this DPA on behalf of itself and, to the extent required under Privacy Laws, its affiliates. Capitalized terms used but not defined in this DPA have the meanings given in the Agreement.

1. Definitions

1.1 "**Aggregated Usage Metrics**" has the meaning given in Section 6.5 of the Agreement.

1.2 "**Authorized Subprocessor**" means a third party engaged by Zipchat to process Personal Data in order to provide the Services, under the general authorization in Section 6.

1.3 "**Zipchat Account Data**" means personal data that relates to Zipchat's relationship with Customer, including the names and contact information of individuals authorized by Customer to access Customer's account, and billing information of individuals that Customer has associated with its account.

1.4 "**Zipchat Usage Data**" means Service usage data collected and processed by Zipchat in connection with the provision of the Services, including data used to identify the source and destination of a communication, activity logs and similar data.

1.5 "**Data Privacy Framework**" or "**DPF**" means, as applicable, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework.

1.6 "**Data Subject**" means a natural person whose Personal Data is protected by Privacy Laws. "Data Subject" includes the term "Consumer" under Privacy Laws.

1.7 "**Data Subject Request**" means a request from a Data Subject to exercise their rights over Personal Data under Privacy Laws.

1.8 "**End User**" means an individual who interacts with the Services on Customer's channels, such as a shopper or website visitor.

1.9 "**EU SCCs**" means the standard contractual clauses approved by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced from time to time, and as completed by Section 9 of this DPA.

1.10 "**ex-EEA Transfer**" means a transfer of Personal Data subject to the EU GDPR from the European Economic Area (the "EEA") to a country or recipient not covered by an adequacy decision of the European Commission.

1.11 "**ex-UK Transfer**" means a transfer of Personal Data subject to the UK GDPR from the United Kingdom (the "UK") to a country or recipient not covered by adequacy regulations made under the UK GDPR and the Data Protection Act 2018.

1.12 "**Personal Data**" means any information provided to Zipchat by or on behalf of Customer, or collected by Zipchat on Customer's behalf in connection with the Services, that relates to an

identified or identifiable Data Subject and constitutes "personal data", "personal information" or an equivalent term under Privacy Laws. Personal Data does not include Zipchat Account Data, Zipchat Usage Data or Aggregated Usage Metrics.

1.13 "**Privacy Laws**" means all laws and regulations applicable to the processing of Personal Data under the Agreement, including, to the extent applicable: (i) Regulation (EU) 2016/679 (the "EU GDPR") and the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR", and together with the EU GDPR, the "GDPR"); (ii) the Swiss Federal Act on Data Protection of 25 September 2020 (the "FADP"); (iii) the UK Data Protection Act 2018; (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (v) U.S. state comprehensive privacy laws, such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the "CCPA"); in each case as amended or replaced from time to time. The terms "business purpose", "Controller", "Personal Data Breach", "Processor", "process" or "processing", "sell", "share" and "supervisory authority" have the meanings given to them, or to equivalent terms, in Privacy Laws. "Controller" includes "Business" and "Processor" includes "Service Provider", as defined in the CCPA.

1.14 "**Standard Contractual Clauses**" means, as applicable, the EU SCCs and the UK SCCs.

1.15 "**Subprocessor List**" means the list of Zipchat's Authorized Subprocessors published at https://www.zipchat.ai/legal/subprocessors, as updated under Section 6.

1.16 "**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, as amended from time to time, and as completed by Exhibit D.

1.17 "**UK SCCs**" means the EU SCCs as amended by the UK Addendum.

2. Role of the Parties; Description of Processing

2.1 With respect to Personal Data, Customer is the Controller and Zipchat is a Processor or, where Customer is a Processor for a third-party Controller, Zipchat is a subprocessor. Zipchat's processing of Zipchat Account Data and Zipchat Usage Data as a Controller is governed by Section 13.

2.2 Zipchat shall process Personal Data only: (i) for the purposes set out in the Agreement; (ii) on Customer's documented instructions, which include the Agreement, this DPA and Customer's configuration and use of the Services; and (iii) as required by Privacy Laws or a supervisory authority, in which case Zipchat shall inform Customer of that legal requirement before processing, unless the law prohibits it. The subject matter, nature, purpose and duration of the processing, the types of Personal Data and the categories of Data Subjects are described in Exhibit A.

2.3 Personal Data is stored in the United States, unless otherwise agreed in writing.

3. Customer's Obligations

3.1 Customer shall, in its use of the Services, process Personal Data and give instructions for its processing in compliance with Privacy Laws, and shall ensure that processing in accordance with its instructions will not cause Zipchat to breach Privacy Laws. Customer is solely responsible for the accuracy, quality and legality of the Personal Data provided to Zipchat by or on behalf of Customer, the means by which Customer acquired it, the instructions it gives to Zipchat, and any notices it must give to, and consents it must obtain from, its End Users.

3.2 Customer shall not provide or make available to Zipchat any Personal Data in breach of the Agreement, including the data described in Section 5.2 of the Agreement, or otherwise

inappropriate for the nature of the Services, and shall indemnify Zipchat against all claims and losses arising from any such data.

3.3 Zipchat shall promptly inform Customer if, in Zipchat's opinion, an instruction infringes Privacy Laws or an instruction of a supervisory authority.

4. Use of Personal Data

4.1 Zipchat shall not: (i) sell or share Personal Data; (ii) retain, use or disclose Personal Data outside the direct business relationship with Customer, or for any purpose other than a business purpose under the CCPA on Customer's behalf or as necessary to perform the Services for Customer under the Agreement, except as otherwise permitted by the Agreement or Privacy Laws; or (iii) combine Personal Data received from or on behalf of Customer with personal data received from or on behalf of another person, except as necessary to provide the Services or as instructed by Customer.

4.2 No training without Customer's authorization. Zipchat does not use Personal Data, including End User conversations, or AI outputs generated from it, to train or fine-tune any AI model, whether Zipchat's own models or third-party models. If Zipchat wants to do so in the future, it will first ask Customer for authorization, by email or in the product, explaining which data would be used and for what purpose. Customer may accept or refuse. Without Customer's express acceptance nothing changes: silence or continued use of the Services is not acceptance. Customer may withdraw an acceptance at any time, with effect for the future. An amendment to the Agreement or to this DPA does not remove or narrow this commitment. Zipchat's AI subprocessors process Personal Data only to provide their service to Zipchat, under contracts that prohibit them from training their models on it. Some may retain limited data for a period, for observability or abuse monitoring. Processing Personal Data to provide the Services to Customer, such as indexing Customer's own content and keeping memory of returning End Users for Customer, is not training.

4.3 Aggregated Usage Metrics. Zipchat may create Aggregated Usage Metrics as described in Section 6.5 of the Agreement. They are combined across customers or across many conversations, do not identify Customer, any Data Subject or any other individual, are not Personal Data, and are never used to train or fine-tune AI models.

4.4 Separation. Zipchat keeps the Personal Data of each customer logically separated, so that it is not exposed in another customer's conversations.

5. Audit

5.1 Zipchat shall maintain records sufficient to demonstrate its compliance with this DPA. On Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Zipchat shall either (i) make available information and documentation reasonably necessary to demonstrate its compliance with this DPA, such as a description of its technical and organizational measures and a summary of the results of its most recent penetration test; or (ii) if the information under (i) is not sufficient under Privacy Laws, allow an independent third-party auditor appointed by Customer to audit Zipchat's data security infrastructure and procedures to the extent necessary to demonstrate compliance with Privacy Laws, provided that: (a) Customer gives reasonable prior written notice and the audit is not unreasonably disruptive to Zipchat's business; (b) the audit takes place during business hours and no more than once per calendar year, unless a supervisory authority requires otherwise or following a Personal Data Breach affecting Customer's Personal Data; and (c) the audit is limited to data relevant to Customer. Customer bears the costs of any audit, including reimbursement of Zipchat's time for on-site audits. Where the Standard Contractual Clauses apply under Section

9, the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 5.1.

5.2 To the extent permitted under Privacy Laws, if Customer determines that Zipchat is processing Personal Data in an unauthorized manner, Customer may, after giving written notice and taking into account the nature of the processing, take commercially reasonable and appropriate steps to stop and remediate the unauthorized processing.

6. Authorized Subprocessors

6.1 General authorization. Customer gives Zipchat general written authorization to engage its affiliates and the Authorized Subprocessors on the Subprocessor List, and to engage further subprocessors under this Section 6, to process Personal Data as necessary to provide the Services.

6.2 Subprocessor List. The current Subprocessor List is published at https://www.zipchat.ai/legal/subprocessors. It shows, for each Authorized Subprocessor, what it processes, where, and whether it is always used or only when Customer enables a feature or connects a channel. Zipchat may add, replace or remove Authorized Subprocessors by updating the Subprocessor List, without amending the Agreement or this DPA. Exhibit B shows the list as at the date of this version, for convenience; the published Subprocessor List controls.

6.3 Notice. At least ten (10) days before a new subprocessor starts processing Personal Data, Zipchat will add it to the Subprocessor List and notify Customer by email to the address on Customer's account. Where an urgent replacement is needed for security or service continuity, Zipchat will give notice as soon as reasonably practicable. Customer can also ask to be notified of every update to the Subprocessor List by writing to support@zipchat.ai.

6.4 Objection. Customer may object to a new subprocessor by writing to support@zipchat.ai within ten (10) days of the notice, on reasonable grounds relating to data protection. If Customer does not object within that period, the subprocessor is an Authorized Subprocessor. The Parties will discuss the objection in good faith. If Zipchat cannot offer a commercially reasonable alternative within a reasonable time, Customer's only remedy is to stop using the affected part of the Services or to terminate the Agreement under its terms. Customer acknowledges that some subprocessors are essential to the Services. Termination under this Section does not relieve Customer of fees owed under the Agreement, and refunds are governed by Section 4.6 of the Agreement.

6.5 Features and channels. Some Authorized Subprocessors process Personal Data only when Customer enables a feature or connects a channel, as shown on the Subprocessor List. By enabling that feature or connecting that channel, Customer instructs Zipchat to use the corresponding Authorized Subprocessor.

6.6 Obligations. Zipchat will enter into a written agreement with each Authorized Subprocessor that imposes data protection obligations no less protective than those imposed on Zipchat under this DPA. Zipchat remains liable to Customer for the performance of each Authorized Subprocessor's obligations, subject to the Agreement.

6.7 Where the Standard Contractual Clauses apply under Section 9: (i) the authorizations in this Section 6 are Customer's prior written authorization to subcontracting under Clause 9 of the EU SCCs; and (ii) copies of subprocessor agreements that Zipchat must provide under Clause 9(c) of the EU SCCs will be provided only on Customer's request, and Zipchat may first remove commercial information and information unrelated to the Standard Contractual Clauses.

7. Confidentiality; Security of Personal Data

7.1 Zipchat shall ensure that every person it authorizes to process Personal Data is bound by an appropriate duty of confidentiality. Zipchat may disclose Personal Data to its advisers, auditors or other third parties as reasonably required to meet its obligations under Privacy Laws, this DPA or the Agreement, or to provide the Services to Customer, subject to equivalent confidentiality obligations.

7.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Zipchat shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as described in Exhibit C. Zipchat may update these measures, provided that updates do not materially reduce the overall level of protection. No method of transmission or storage is completely secure, and Zipchat does not guarantee absolute security.

8. Personal Data Breach

8.1 Zipchat shall inform Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer's Personal Data, and shall take the steps it reasonably considers necessary to contain and remediate it, to the extent remediation is within Zipchat's reasonable control. The notice will describe, to the extent then known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, its likely consequences and the measures taken or proposed.

8.2 Taking into account the nature of the processing and the information available to it, Zipchat shall give Customer reasonable cooperation and assistance so that Customer can meet its obligations under Privacy Laws to notify the relevant supervisory authority and affected Data Subjects.

8.3 Sections 8.1 and 8.2 do not apply to a Personal Data Breach caused by the acts or omissions of Customer or its users. Zipchat's notice of or response to a Personal Data Breach is not an acknowledgment of fault or liability.

9. Transfers of Personal Data

9.1 Customer acknowledges that Zipchat's primary processing operations, and its Authorized Subprocessors' processing of Personal Data, take place in the United States, and that transferring Personal Data to the United States is necessary to provide the Services. Zipchat may transfer Personal Data outside the EEA, the UK or Switzerland as necessary to provide the Services, with the safeguards required by Privacy Laws.

9.2 Data Privacy Framework. Zipchat Inc. is certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework. Its certification is listed at https://www.dataprivacyframework.gov/list. Transfers of Personal Data from the EEA to Zipchat are therefore covered by the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework of 10 July 2023, and transfers from the UK and Switzerland by the corresponding UK and Swiss adequacy findings for the DPF. For these transfers, Standard Contractual Clauses and a transfer impact assessment are not required. Zipchat shall notify Customer if it can no longer meet its obligations under the DPF Principles.

9.3 Fallback mechanism. The Standard Contractual Clauses are incorporated into this DPA by reference and apply to an ex-EEA Transfer, an ex-UK Transfer or a transfer from Switzerland only: (a) if the Data Privacy Framework ceases to be a valid transfer mechanism for that

transfer, or Zipchat's certification lapses; or (b) if Customer asks in writing that they apply as an additional safeguard. Where they apply, they are completed as follows:

(a) Module Two (controller to processor) applies where Customer is a Controller and Zipchat is a Processor; Module Three (processor to processor) applies where Customer is a Processor and Zipchat is a subprocessor; and Module One (controller to controller) applies to Zipchat Account Data and Zipchat Usage Data that Zipchat processes as a Controller under Section 13.

(b) The optional docking clause in Clause 7 does not apply.

(c) In Clause 9, Option 2 (general written authorization) applies, and the time period for prior notice of subprocessor changes is the one set out in Section 6.3.

(d) In Clause 11, the optional language does not apply.

(e) In Clause 13, the competent supervisory authority is determined as set out in Exhibit B.

(f) In Clause 17 (Option 1), the EU SCCs are governed by the laws of Ireland, and under Clause 18(b) disputes are resolved before the courts of Ireland.

(g) Annex I is completed by Exhibits A and B, Annex II by Exhibit C, and Annex III by the Subprocessor List.

(h) By accepting the Agreement, the Parties are deemed to have signed the EU SCCs, including their Annexes, as of the date Customer accepted the Agreement.

9.4 ex-UK Transfers. Where Section 9.3 applies to an ex-UK Transfer, the UK SCCs apply, completed as set out in Exhibit D. The UK Addendum is governed by the laws of England and Wales, and disputes arising from it are resolved by the courts of England and Wales.

9.5 Transfers from Switzerland. Where Section 9.3 applies to a transfer subject to the FADP, the EU SCCs apply with these changes: (a) references to the GDPR include the FADP for those transfers; (b) the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for transfers governed by the FADP; and (c) the term "Member State" does not prevent Data Subjects in Switzerland from bringing claims in their place of habitual residence under Clause 18(c).

9.6 Government access requests. For any transfer made under the Standard Contractual Clauses: (a) as of the date of this version, Zipchat has not received any legally binding request from a government intelligence or security agency for access to Customer Personal Data; (b) if Zipchat receives a request from a public authority for Personal Data, it shall try to redirect the authority to Customer, for which purpose it may provide Customer's basic contact information, and, where it is compelled to disclose Personal Data, shall notify Customer to the extent legally permitted and reasonably cooperate so that Customer can seek a protective order or other remedy; (c) Zipchat shall not voluntarily disclose Personal Data to a law enforcement or government authority; and (d) if a transfer mechanism ceases to be valid or a supervisory authority requires transfers to be suspended, the Parties shall agree on an alternative mechanism that complies with Privacy Laws.

10. Data Protection Assessments

10.1 Taking into account the nature of the processing and the information available to it, Zipchat shall reasonably cooperate with Customer in any data protection impact assessment or prior consultation required by Privacy Laws, including by providing information that Customer cannot otherwise obtain. Each Party remains responsible for the measures allocated to it under Privacy Laws.

11. Data Subject Requests

11.1 To the extent permitted by Privacy Laws, Zipchat shall notify Customer if it receives a Data Subject Request relating to Personal Data, and shall advise the Data Subject to submit the request to Customer. Customer is responsible for responding to Data Subject Requests, including by using the functionality of the Services, such as deleting or exporting conversation data.

11.2 At Customer's request, and taking into account the nature of the processing, Zipchat shall assist Customer with appropriate technical and organizational measures in responding to a Data Subject Request, where Customer cannot respond without Zipchat's assistance and Zipchat can lawfully do so. To the extent legally permitted, Customer is responsible for reasonable costs of that assistance.

12. Retention, Return and Deletion of Personal Data

12.1 **During the subscription.** Zipchat keeps Personal Data, including conversation data, for as long as Customer's subscription is active, so that Customer can access it and the AI agent can keep memory of returning End Users. Conversations are not deleted automatically while the subscription is active. Customer may delete conversation history at any time, and may ask support@zipchat.ai to enable automatic deletion after a period Customer chooses, which Zipchat will apply within a reasonable time.

12.2 **Export.** Customer may export conversation data through the Zipchat API at no additional cost while its account is active and for 90 days after termination, until the data is deleted, through the API or by contacting support@zipchat.ai.

12.3 **After termination.** Zipchat will delete Personal Data within 90 days of termination or expiry of the Agreement, subject to backup cycles, except where further storage is required by law or needed for billing, tax or legal records. Personal Data that Zipchat retains under this exception remains protected under this DPA and is not processed further except as the law requires.

12.4 Where the Standard Contractual Clauses apply, the certification of deletion described in Clauses 8.1(d) and 8.5 of the EU SCCs will be provided on Customer's request.

13. Zipchat as a Controller

13.1 For Zipchat Account Data and Zipchat Usage Data, Zipchat is an independent Controller, not a joint controller with Customer. Zipchat processes this data: (i) to manage its relationship with Customer; (ii) to carry out its core business operations, such as accounting, audits, tax and compliance; (iii) to monitor, investigate, prevent and detect fraud, security incidents and misuse of the Services; (iv) to verify identity; (v) to comply with its legal obligations; (vi) to provide, secure, maintain and improve the Services, including by creating Aggregated Usage Metrics; and (vii) as otherwise permitted by Privacy Laws, the Agreement and this DPA. Zipchat does not use conversation content contained in this data to train or fine-tune AI models. This processing is described in Zipchat's Privacy Policy at https://www.zipchat.ai/legal/privacy-policy.

14. Changes to this DPA

14.1 Zipchat may update this DPA, for example to reflect changes in Privacy Laws, transfer mechanisms or the Services, by publishing the updated version on its website. Changes that materially reduce Customer's protections take effect 30 days after Zipchat notifies Customer by email, unless Privacy Laws require them sooner. Changes to the Subprocessor List follow Section 6, not this Section. No update may remove or narrow the commitment in Section 4.2.

15. Miscellaneous

15.1 In case of conflict, the following order of precedence applies: (1) the Standard Contractual Clauses, where they apply under Section 9; (2) this DPA; (3) Zipchat's Privacy Policy, as regards the processing of personal data, consistent with Section 6.4(d) of the Agreement; and (4) the Agreement.

15.2 Any claim brought in connection with this DPA is subject to the Agreement, including its governing law and the exclusions and limitations of liability in the Agreement, except where the Standard Contractual Clauses provide otherwise.

15.3 Notices to Zipchat under this DPA must be sent to support@zipchat.ai. Notices to Customer are sent to the email address on Customer's account.

15.4 This DPA is written in English. Any translation, including AI-assisted translations published on Zipchat's website, is provided for convenience only and may contain errors. The English version is the only binding version and prevails in case of any conflict, including in any dispute, arbitration or court proceeding.

Exhibit A: Details of Processing

Subject matter. The provision of the Services under the Agreement: an AI agent for ecommerce that answers and assists Customer's End Users across the channels Customer connects, such as website chat, search, product pages, email, WhatsApp, Instagram, Messenger and, where enabled, voice.

Nature of processing. Collection, recording and retrieval; storage and structuring; analysis and consultation, including generating AI replies; indexing of Customer's content; updating and correction; protection, including encryption and restriction; disclosure to Authorized Subprocessors and to the tools Customer connects; return to Customer or Data Subjects; and erasure.

Purpose. To provide, maintain, secure and support the Services for Customer under the Agreement and Customer's instructions. Personal Data is not used to train or fine-tune AI models without Customer's authorization (Section 4.2).

Duration. For the term of the Agreement and as set out in Section 12: Personal Data is kept while the subscription is active, unless Customer deletes it or enables automatic deletion, and is deleted within 90 days of termination, subject to backup cycles and the exceptions in Section 12.3.

Categories of Data Subjects. Customer's End Users (shoppers and website visitors who interact with the Services), and Customer's personnel and authorized users of the Services.

Categories of Personal Data.

- Contact details, such as name, email address and phone number.
- Messaging identifiers, such as WhatsApp phone numbers and Instagram and Messenger profile IDs, where Customer connects those channels.
- Conversation content: chat messages, emails, enquiries and support requests, and media End Users send, such as images and voice notes.
- Order and purchase information retrieved from Customer's connected platforms, such as order numbers, order status and order history.
- Information returned by custom tools or skills that Customer configures, which can include order and customer data.
- Technical data, such as IP address, approximate location, and browser and device information, including signals used for bot checks where Customer enables bot protection.
- For Customer's users: name, email address, role and account activity.

Special categories of data. Zipchat never asks End Users for special categories of personal data. An End User may volunteer such data, for example a pregnancy or an allergy when asking about a product, because a safe and relevant answer depends on it. By design, Zipchat does not mask this data automatically: removing it before the AI model sees it would make the answer worse or unsafe. It is processed only to answer that End User, sent only to the AI subprocessors on the Subprocessor List, all in the United States, encrypted in transit and at rest, never used to train AI models, and filtered out of Zipchat's application logs. Customer can delete the conversation at any time. Customer shall not use the Services to collect special categories of data on purpose, nor the data excluded by Section 5.2 of the Agreement.

Frequency. Continuous, for as long as Customer uses the Services.

Exhibit B: Parties, Description of Transfer and Subprocessors

This Exhibit contains the information required by Annexes I and III of the EU SCCs and by Table 1 and Annexes 1A and 1B of the UK Addendum, where they apply under Section 9.

1. The Parties

Data exporter: Customer, as identified in its Zipchat account. Contact details: those on Customer's account. Activities relevant to the transfer: use of the Services under the Agreement. Role: Controller or Processor, as set out in Section 2. Signature and date: by accepting the Agreement, Customer is deemed to have signed, as of the date of acceptance.

Data importer: Zipchat Inc., 407 E Ayre St #1207, Wilmington, Delaware DE 19804, United States. Contact: support@zipchat.ai. Activities relevant to the transfer: provision of the Services under the Agreement. Role: Processor (or subprocessor), and Controller for Zipchat Account Data and Zipchat Usage Data under Section 13. Signature and date: by providing the Services under the Agreement, Zipchat is deemed to have signed, as of the date Customer accepted the Agreement.

2. Description of the Transfer

Item	Description
Categories of Data Subjects	As described in Exhibit A.
Categories of Personal Data	As described in Exhibit A.
Special categories of data	As described in Exhibit A.
Nature and purpose of processing	As described in Exhibit A.
Duration and retention	As described in Exhibit A and Section 12.
Frequency of the transfer	Continuous, as needed to provide the Services.
Recipients	The Authorized Subprocessors on the Subprocessor List.

3. Competent Supervisory Authority

The supervisory authority of the data exporter, determined under Clause 13 of the EU SCCs. Where the data exporter has no establishment in the EEA and has appointed a representative, the supervisory authority of the Member State where the representative is established. For the UK Addendum, the UK Information Commissioner. For transfers subject to the FADP, the Swiss Federal Data Protection and Information Commissioner.

4. Authorized Subprocessors

The current list is the Subprocessor List at https://www.zipchat.ai/legal/subprocessors, which controls and may be updated under Section 6. At the date of this version (12 November 2026), it includes the following. All process data in the United States.

Used for every customer

Subprocessor	Category	What it processes
Heroku (Salesforce)	Hosting	App servers, workers, database (chats, conversations, messages, leads, pages, configuration, billing), background job data
AWS S3	Storage	Inbound email and archive, archived data, search index import files
Cloudinary	Storage	Chat attachments: shopper images, voice notes, email and social media images
Pinecone	Vector	Embeddings of merchant site and product content, price data

Subprocessor	Category	What it processes
	database	
Google Gemini	AI	Conversation content, tool results, product images, site page indexing, embeddings
Microsoft Azure OpenAI	AI	Conversation content and tool results (fallback model for every conversation)
OpenAI	AI	Embeddings of merchant content, conversation content, tool calls
AWS Bedrock	AI	Conversation content, tool calls
Anthropic	AI	Conversation content, tool calls
Meta AI (LLM models)	AI	Conversation content, tool calls
ElevenLabs	AI	Conversation content, tool calls
TypeSafe	AI	Conversation content, tool calls
Cloudflare	Network and security	All traffic to and from Zipchat, over HTTPS (content delivery, DNS and protection)
New Relic	Monitoring	Performance traces and app events
Segment	Analytics	Merchant user and account events
Amplitude	Analytics	Dashboard product analytics (merchant users)
Customer.io	Lifecycle email	Merchant user emails and lifecycle events
Attio	CRM	Merchant accounts, users and AI agents
Slack	Internal alerts	Merchant account and plan updates
Beehiiv	Marketing pixel	Visits to signup, onboarding and dashboard pages
OpenAI Ads	Marketing pixel	Visits to signup, onboarding and dashboard pages

Used when a feature applies

Subprocessor	Category	What it processes	When it applies
Shopify Billing	Payments	Subscription charges and install state	The store is on Shopify and billed through Shopify
Stripe	Payments	Customer, subscription and payment data	The merchant is billed through Stripe (stores not on Shopify)
Meta (WhatsApp, Messenger, Instagram)	Messaging	Shopper messages, phone numbers, profile IDs, media	The merchant connects WhatsApp, Messenger or Instagram
Zendesk	Support	Escalated conversations and shopper contact details	The merchant connects the Zendesk channel
Cloudflare	Security	Shopper IP address and browser signals for bot checks	The merchant turns on bot protection (off by default)
E2B	Infrastructure	Custom tool inputs and API responses, which can include order and customer data	The merchant uses custom tools or skills, or connects a codebase

Exhibit C: Technical and Organizational Measures

This Exhibit contains the information required by Annex II of the EU SCCs and Annex II of the UK Addendum, where they apply under Section 9. Zipchat implements the following measures to protect Personal Data against unauthorized access, disclosure, alteration and loss.

- **Encryption.** All data is encrypted at rest, including database storage, file storage and backups. All traffic is encrypted in transit: every connection runs over HTTPS through Cloudflare, and database connections are encrypted. Selected sensitive integration credentials, such as access tokens, database passwords and custom skill secrets, also receive application-level encryption at rest, and custom skill secret values are write-only through the API.
- **Access control.** The customer application requires authentication. Role-based permissions distinguish owners, editors, members and administrators and restrict sensitive functions. Internal tools are limited to authorized administrators. Passwords are stored only as salted hashes.
- **Customer data separation.** Personal Data is logically associated with the customer's workspace and AI agent. Application access is scoped to the agents a user can access, and knowledge-base searches use agent-specific namespaces, to prevent access across customer accounts.
- **Secure integrations.** External service integrations use HTTPS and authenticated API requests. Shopify webhooks are verified by signature, and backend API credentials are checked with constant-time comparison.
- **Logging and monitoring.** Errors and system activity are monitored continuously, with error reporting and application performance monitoring. Secrets and message content are filtered out of logs, and detailed error pages are disabled in production.
- **Backups and resilience.** Zipchat keeps regular database backups. Background processing retries recoverable failures, deployment procedures are designed to reduce service interruption, and a database-enforced read-only access mechanism is available for operational investigation.
- **Development and change management.** Every code change is kept in version control and goes through review and automated tests before it is deployed, with staging verification before production.
- **Vulnerability management.** Zipchat runs regular penetration tests and keeps an ongoing vulnerability management process for its application and its dependencies.
- **Data lifecycle.** Customers can delete conversations, agents and indexed knowledge-base data at any time, and can ask support to enable automatic deletion of conversations after a chosen period. Zipchat deletes Personal Data within 90 days of termination, subject to backup cycles (Section 12).
- **Purpose limitation.** Personal Data is processed only on Customer's instructions to provide the Services. It is not used for advertising and is not used to train or fine-tune any AI model without Customer's authorization (Section 4.2).
- **Subprocessors.** Zipchat engages subprocessors under written agreements with data protection obligations no less protective than this DPA, and AI subprocessors under terms that prohibit training on Personal Data (Section 6).

Exhibit D: UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses. This Exhibit applies only where the UK SCCs apply under Sections 9.3 and 9.4.

Part 1: Tables

Table 1: Parties

	Exporter	Importer
Start date	The date the UK SCCs start to apply under Section 9.3	Same
Parties' details	Customer	Zipchat Inc.
Key contact	See Exhibit B	See Exhibit B

Table 2: Selected SCCs, Modules and Clauses. The version of the approved EU SCCs to which this UK Addendum is appended, as incorporated into the DPA and completed by Section 9.3.

Table 3: Appendix information. Annex 1A (list of parties): Exhibit B. Annex 1B (description of transfer): Exhibits A and B. Annex II (technical and organizational measures): Exhibit C. Annex III (list of subprocessors, Modules 2 and 3): the Subprocessor List.

Table 4: Ending this UK Addendum when the approved UK Addendum changes. Either the Importer or the Exporter may end this UK Addendum as set out in Section 19 of the UK Addendum.

Part 2: Mandatory Clauses

The Mandatory Clauses of the approved UK Addendum, as issued by the UK Information Commissioner and amended from time to time, are incorporated by reference.