ZIP DATA PROCESSING POLICY

This Data Processing Policy provides additional terms that apply where Zip Processes Personal Data as a Processor on behalf of Customer when providing the Solution to Customer pursuant to the Zip Master Subscription Agreement ("**Agreement**"). Zip may update or change this agreement from time to time but will never materially decrease the level of security or privacy rights as set out in this Data Processing Policy.

SECTION I - DEFINITIONS

Unless otherwise defined herein, all capitalized terms have the meaning given to them in, the Zip Information Security Policy (available at https://assets.ziphq.com/legal/zip-information-security-06-2024.pdf) or in the body of the Agreement.

"CCPA" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Subject" means the individual to whom Personal Data relates.

"Data Protection Laws" means, to the extent they are applicable, (a) the UK GDPR; (b) the GDPR; the FADP; and (c) the CCPA.

"FADP" means the Swiss Federal Act on Data Protection.

"GDPR" means the General Data Protection Regulation ((EU) 2016/679), as it has effect in EU law.

"**Process**" or **Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" means the entity which processes Personal Data on behalf of the Controller.

"**SCCs**" means, where the GDPR applies, the Controller to Processor Standard Contractual Clauses adopted under the GDPR available at https://assets.ziphq.com/legal/gdpr-c2p-sccs.pdf ("**EU Controller to Processor SCCs**"), and, where the UK GDPR applies, the International Data Transfer Addendum incorporating the EU Controller to Processor SCCs available at https://assets.ziphq.com/legal/zip-UK-IDTA-Addendum.pdf ("**UK IDTA Addendum**").

"**Subprocessor**" means a third-party entity engaged by Zip as a Data Processor under this Data Processing Policy.

"Restricted Transfer" means (a) to the extent that the GDPR applies to the processing, a country outside the European Economic Area not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR); (b) to the extent the UK GDPR applies to the processing, a country outside the United Kingdom not recognized by the UK Government as providing an adequate level of protection for personal data (as described in the UK-GDPR), or (c) to the extent that FADP applies to the processing, a county outside Switzerland not recognized as providing an adequate level of protection for personal data (as described in the FADP).

"UK GDPR" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

Clause 1

Purpose and Scope

a. The purpose of this Data Processing Policy is to ensure compliance with the Data Protection Laws as they may be amended, replaced, or supplemented from time to time.

b. Customer and Zip have agreed to this Data Processing Policy to ensure compliance with the Data Protection Laws.

c. This Data Protection Policy applies to the Processing of Personal Data as specified in Annex II.

d. Annexes I to III are an integral part of this Data Processing Policy.

e. This Data Processing Policy is without prejudice to obligations to which Customer is subject by virtue of the Data Protection Laws.

f. To the extent that the Processing of Personal Data is within the scope of the CCPA, (a) Customer shall be considered the "Business" and Zip shall be considered the "Service Provider" and (b) "business purpose", "commercial purpose", "personal information", "sell", and "share" shall have the meanings given in the CCPA.

Clause 2

Interpretation

a) This Data Processing Policy shall be read and interpreted in the light of the provisions of the Data Protections Laws, to the extent that they apply.

b) This Data Processing Policy shall not be interpreted in a way that runs counter to the rights and obligations provided for in the Data Protection Laws or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

Clause 3

Hierarchy

In the event of a contradiction between this Data Processing Policy and the provisions of related agreements between the parties existing at the time when this Data Processing Policy is agreed or entered into thereafter, this Data Processing Policy shall prevail.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 4

Description of Processing

The details of the Processing, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of Customer, are specified in Annex II.

Clause 5

Obligations of the Parties

5.1 Instructions

a. Zip shall Process Personal Data only on documented instructions from Customer, unless required to do so by applicable local law to which Zip is subject. In this case, Zip shall inform Customer of that legal requirement before Processing, unless the law prohibits this. Subsequent instructions may also be given by Customer throughout the duration of the Processing of Personal Data. These instructions shall always be documented.

b. Zip shall immediately inform Customer if, in Zip's opinion, instructions given by the Customer infringe the Data Protection Laws or the applicable local law data protection provisions.

c. To the extent that the Processing of Personal Data is within the scope of the CCPA, the following additional terms shall apply:

1. Zip shall not sell or share Personal Data.

2. Zip shall not retain, use, or disclose Personal Data for:

   A. any purposes, including any business purposes, other than to perform the services specified in the Agreement, or as otherwise required under applicable law; or

   B. outside of the direct business relationship between Zip and Customer.

3. Zip shall not combine Personal Data with any other personal information it receives from another source, except as permitted by under the CCPA.

4. Zip will comply with the applicable obligations under the CCPA and provide the same level of privacy protection to Personal Data as required by the CCPA.

5. Zip shall promptly notify Customer if it makes a determination that it can no longer meet the obligations under the CCPA.

5.2. Purpose limitation

Zip shall process Personal Data only for the specific purpose(s) of the Processing, as set out in Annex II, unless it receives further instructions from Customer.

5.3. Duration of the Processing of Personal Data

Processing by Zip shall only take place for the duration specified in Annex II.

5.4. Security of Processing

a. Zip shall at least implement the technical and organizational measures specified in Annex III to ensure the security of Personal Data. This includes protecting Personal Data against a Data Breach. In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for Data Subjects.

b. Zip shall grant access to Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the Agreement. Zip shall ensure that persons authorized to Process Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.5. Sensitive Data

If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**Sensitive Data**"), Zip shall apply specific restrictions and/or additional safeguards. The collection of Sensitive Data is prohibited under the Agreement.

5.6. Documentation and Compliance

a. The parties shall be able to demonstrate compliance with this Data Processing Policy.

b. Zip shall deal promptly and adequately with inquiries from Customer about the Processing of Personal Data in accordance with this Data Processing Policy.

c. Zip shall make available to Customer all information necessary to demonstrate compliance with the obligations that are set out in this Data Processing Policy and/or stem directly from the Data Protection Laws. At Customer's request, Zip shall also permit and contribute to audits of the Processing activities covered by this Data Processing Policy, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, Customer may take into account relevant certifications held by Zip.

d. Customer may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of Zip if mutually agreed and shall, where appropriate, be carried out with reasonable notice.

e. The parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

f. Customer chooses to conduct any audit or inspection it has the right to request or mandate on its own behalf by instructing Zip to carry out an audit in accordance with the terms of Section 7 (Audits) of the Zip Information Security Policy. If Customer wishes to change this instruction regarding the audit or inspection, Customer has the right to request a change to this instruction by sending Zip written notice as provided for in the Agreement. If Zip declines to follow any such instruction requested by Customer regarding audits, including inspections, and should the parties fail to mutually agree on a reasonable alternative to such request within 15 business days following Zip's decision to decline such request, Customer is entitled to terminate the Agreement in accordance with its terms.

5.7. Use of Subprocessors

a. Zip has Customer's general authorization for the engagement of Subprocessors posted on https://ziphq.com/subprocessors. Customer may subscribe on that webpage to be notified of any intended changes of that list through the addition or replacement of Subprocessors at least ten days in advance.

b. Where Zip engages a Subprocessor for carrying out specific Processing activities (on behalf of Customer), it shall do so by way of a contract which imposes on the Subprocessor, in substance, the same data protection obligations as the ones imposed on Zip in accordance with this Data Processing Policy. Zip shall ensure that the Subprocessor complies with the obligations to which Zip is subject pursuant to this Data Processing Policy and to the Data Protection Laws.

c. At the Customer's request, Zip shall provide a copy of such a Subprocessor agreement and any subsequent amendments to Customer. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Zip may redact the text of the agreement prior to sharing the copy.

d. Zip shall remain fully responsible to Customer for the performance of the Subprocessor's obligations in accordance with its contract with Zip. Zip shall notify Customer of any material failure by the Subprocessor to fulfil its contractual obligations to process Customer's Personal Data in accordance with this Data Processing Policy.

e. This Clause 5.7(e) shall apply only where the GPDR or the UK GDPR applies to the Processing of the Personal Data:

1. Customer may object to Zip's use of a new Subprocessor on reasonable grounds related to the protection of the Personal Data by notifying Zip in writing within ten business days after notice of an updated Subprocessor List. In that event, Zip shall use commercially reasonable efforts to make available to Customer a change in the Solution or recommend a commercially reasonable change to Customer's use of the Solution to avoid Processing of Personal Data by the objected-to new Subprocessor. Any change to Customer's use of the Solution must not unreasonably burden Customer.

2. If Zip is unable to make such change within a reasonable period of time and the parties cannot come to a mutually agreed upon solution, Customer may give written notice to terminate those parts of the Solution which cannot be provided by Zip without the use of the objected-to new Subprocessor. Promptly following termination, Zip shall provide a pro-rata refund of the license fees that have been paid in advance for the remainder of the Subscription Term for the applicable Solution, calculated from the date of termination.

3. Zip shall agree a third-party beneficiary clause with the Subprocessor whereby in the event Zip has factually disappeared, ceased to exist in law or has become insolvent - the Customer shall have the right to terminate the Subprocessor contract and to instruct the Subprocessor to erase or return the Personal Data.

5.8. International Transfers

a. This Clause 5.8 shall apply only where the GDPR or the UK GDPR applies to Zip's Processing of the Personal Data.

b. Any Restricted Transfer, either directly or via onward transfer, of Personal Data or transfer to an international organization by Zip shall be done only on the basis of documented instructions from Customer or in order to fulfil a specific requirement under applicable local law to which Zip is subject and shall take place in compliance with the GDPR, the UK-GDPR, or FADP (as applicable). Zip may transfer Personal Data to its Affiliates or its Subprocessors through a Restricted Transfer, subject to the notification requirements of Clause 5.7.

c. Customer agrees that where Zip engages a Subprocessor in accordance with Clause 5.7. for carrying out specific Processing activities (on behalf of the Customer) and those Processing activities involve a transfer of Personal Data, either directly or via onward transfer, or via Restricted Transfer, Zip and the Subprocessor can ensure compliance with the GDPR, the UK-GDPR, or FADP (as applicable) using the relevant SCCs, provided the conditions for the use of those SCCs are met. The parties shall use reasonable efforts to agree any relevant changes to the SCCs, or replacement clauses, including sharing relevant information to complete any applicable transfer risk assessments, to enable the continued transfer of Personal Data as intended by the parties under this Agreement.

d. The SCCs shall apply between Customer and Zip only when Personal Data is transferred, either directly or via onward transfer, and is subject to a Restricted Transfer. When Zip or its Sub-processors are certified under the EU-US Data Privacy Framework and its extensions, the Parties agree that transfers to such entities are not considered a Restricted Transfer. When this Clause 5.8 (d) applies, the following terms shall also apply:

1. For the purposes of Clauses 5.8(d)(1)-(7), references to the "SCCs" means: where GDPR or FADP applies the EU Controller to Processor SCCS; and where UK GDPR applies the Addendum EU SCCs (as defined in the UK IDTA Addendum).

2. For the purposes of Clause 8.5 (Duration of processing and erasure or return of data) of the SCCs, data erasure and return shall be performed in accordance with the terms of the Section 8.6 (Return of Data) and Section 8.7 (Data Disposal) of the Zip Information Security Policy.

3. For the purposes of Clause 8.6 (c) and (d) (Security of processing) of the SCCs, data breaches shall be managed in accordance with the terms of Section 10 (Data Breaches) of Zip Information Security Policy.

4. For the purposes of Clause 8.9 (Documentation and compliance) of the SCCs, audits shall be performed in accordance with the terms of Section 7 (Audits) of Zip Information Security Policy.

5. For the purposes of Clause 9 (Subprocessors) of the SCCs, Subprocessors shall be managed in accordance with the terms of Section 5.7 (Use of Subprocessors) of this Data Processing Policy.

6. For purposes of Clause 12 (Liability) of the SCCs, liability of a party to the other party for breach of this Data Processing Policy shall be subject to the terms of Section 12 (Limitation of Liability) of the Agreement, to the extent permitted by law.

7. For purposes of Clause 15 (Obligations of the data importer in case of access by public authorities) of the SCCs, requests shall be managed in accordance with Zip's Government Data Request Policy (available at https://assets.ziphq.com/legal/Zip_Government_Access_Request_Policy.pdf)

8. For purposes of Clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction) of the SCCs, the governing law, forum and jurisdiction named therein (and where UK GDPR applies, the governing law, forum and jurisdiction named in the UK IDTA Addendum) shall apply to the SCCs and the Agreement, including this Data Processing Policy, to give full effect to the Agreement in respect of the enforcement of any rights or obligations, or any claims under the SCCs or the UK IDTA.

e. Where Personal Data is protected by the FADP, the EU Controller to Processor SCCS as set forth in Clause 5.8(d) shall apply with the following modifications:

1. For the purposes of Clause 13 (), the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

2. For purposes of Clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction), the governing law, forum and jurisdiction shall be Switzerland and the courts of Switzerland, and the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

3. For the purposes of Clause 13 (Supervision), the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

4. All references to the EU Controller to Processor SCCS in this Data Processing Policy are also deemed to refer to the FADP.

f. The parties agree that the terms of this Clause 5.8 are not intended to amend or modify the SCCs. These provisions provide clarity in terms of Zip's business processes for complying with the SCCs. In the event of any conflict between the terms of this Data Processing Policy and the provisions of the SCCs, the SCCs shall prevail.

Clause 6

Assistance to the Customer

a. Zip shall promptly notify Customer of any request it receives from Data Subjects. It shall not respond to the request itself, unless authorized to do so by Customer.

b. Zip shall assist Customer in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the Processing. In fulfilling its obligations in accordance with (a) and (b), Zip shall comply with Customer's instructions.

c. In addition to Zip's obligation to assist Customer pursuant to Clause 6(b), Zip shall furthermore assist Customer in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to Zip:

1. The obligation to carry out an assessment of the impact of the envisaged Processing on the protection of Personal Data (a "**Data Protection Impact Assessment**") where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

2. the obligation to consult the competent supervisory authority/ies prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk;

3. the obligation to ensure that Personal Data is accurate and up to date, by informing Customer without delay if Zip becomes aware that Personal Data it is Processing is inaccurate or has become outdated;

4. the obligations in the Data Protection Laws.

d. The parties shall set out in Annex III the appropriate technical and organizational measures by which Zip is required to assist Customer in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 7

Notification of Data Breach

In the event of a Data Breach, Zip shall cooperate with and assist the Customer for the Customer to comply with its obligations under the Data Protection Laws, taking into account the nature of Processing and the information available to Zip.

7.1 Data Breach concerning Personal Data Processed by the Customer

a. In the event of a Data Breach concerning Personal Data Processed by the Customer, Zip shall assist the Customer:

1. in notifying the Data Breach to the competent supervisory authority/ies, without undue delay after Customer has become aware of it, where relevant and unless the Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons;

2. in obtaining the following information which, pursuant to the Data Protection Laws, shall be stated in Customer's notification, and must at least include:

A. the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

B. the likely consequences of the Data Breach;

C. the measures taken or proposed to be taken by Customer to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

b. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c. In complying, pursuant to the Data Protection Laws, with the obligation to communicate without undue delay the Data Breach to the Data Subject, when the Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

7.2 Data Breach Concerning Personal Data Processed by Zip

a. In the event of a Data Breach concerning Personal Data processed by Zip, Zip shall notify Customer in accordance with the terms of Section 10 (Data Breaches) of the Zip Information Security Policy.

b. The parties shall set out in Annex III all other elements to be provided by Zip when assisting Customer in the compliance with Customer's obligations under the Data Protection Laws.

SECTION III - FINAL PROVISIONS

Clause 8

Non-Compliance with this Data Processing Policy and Termination

a. This Data Processing Policy will continue in force until the termination of the Agreement.

b. Without prejudice to any provisions of the Data Protection Laws, in the event that Zip is in breach of its obligations under this Data Processing Policy, Customer may instruct Zip to suspend the Processing of Personal Data until the latter complies with

this Data Processing Policy or the Agreement is terminated. Zip shall promptly inform Customer in case it is unable to comply with this Data Processing Policy, for whatever reason.

c. Customer shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data in accordance with this Data Processing Policy if:

    1. The Processing of Personal Data by Zip has been suspended by the Customer pursuant to point (a) and if compliance with this Data Processing Policy is not restored within a reasonable time and in any event within one month following suspension or another mutually agreed time period;

    2. Zip is in substantial or persistent breach of this Data Processing Policy or its obligations under the Data Protection Laws;

    3. Zip fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Data Processing Policy or to the Data Protection Laws.

d. Zip shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data under this Data Processing Policy where, after having informed Customer that its instructions infringe applicable legal requirements in accordance with Clause 5.1 (b), Customer insists on compliance with the instructions.

e. Following termination of the Agreement, Zip shall delete all Personal Data processed on behalf of Customer in accordance with the terms of Section 8.7 (Data Disposal) of the Zip Information Security Policy, unless applicable local law requires storage of the Personal Data, and certify to Customer that it has done so, at Customer's request. Prior to termination of the Agreement, Customer may export their Personal Data in accordance with the terms of Section 8.6 (Return of Data) of the Zip Information Security Policy. Until the Personal Data is deleted or returned, Zip shall continue to ensure compliance with this Data Processing Policy.

ANNEX I

List of parties

Controller: Customer

For Customer details and accession date refer to the named “Customer” on the signed or accepted Order Form or Agreement.

Processor: Zip

For Zip details and accession date refer to “Zip” on the signed or accepted Order Form or Agreement.

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

The Customer has sole control over the categories of data subjects whose personal data may be imported into Zip's Solution.

Categories of personal data processed

- Full name
- Name of employer
- Job title
- Email address
- Physical address
- Telephone number
- Purchase and usage history IT information, such as IP address

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Sensitive personal data is restricted from upload into Zip's Solution

Nature of the processing

The nature and purpose of the Processing is Zip's provision of the Solution. Zip provides procurement workflows and processes business data at each step. Administrators create workflow templates upon which users can create purchase requests. Zip orchestrates each workflow, from intake to approval, and provides insights and a management layer for administrators.

Purpose(s) for which the personal data is processed on behalf of the Customer

To provide the Solution.

Duration of the processing

For the Subscription Term and for up to 30 days after until deleted in accordance with Section 8.7 (Data Disposal) of the Zip Information Security Policy.

For processing by Subprocessors, also specify subject matter, nature and duration of the processing

Please see https://ziphq.com/subprocessors for details on Subprocessors.

ANNEX III

Technical and organizational measures including technical and organizational measures to ensure the security of the data

A description of the information security controls implemented by Zip to protect personal data is set forth in the Zip Information Security Policy available at https://assets.ziphq.com/legal/zip-information-security-06-2024.pdf.