



Last Updated: April 24, 2026

DATA PROCESSING AGREEMENT

If you, the Customer, require a mutually executed copy of this Data Processing Agreement (this “**DPA**”), please email a completed copy to privacy@zasio.com. No changes made to this DPA are agreed to by Zasio Enterprises, Inc. (“**Zasio**”).

This DPA is entered into between the contracting Customer, and Zasio (each a “**Party**” and collectively, the “**Parties**”).

This DPA is incorporated into and forms part of the governing master agreement between Customer and Zasio pursuant to which Personal Data is being Processed (the “**Agreement**”). Capitalized terms not defined in this DPA have their meanings derived in the Agreement. This DPA, in conjunction with Zasio’s commitments in the Agreement, are Zasio’s only responsibility with respect to the Processing of Personal Data under the Agreement.

In case of a conflict between this DPA and the Agreement, this DPA will prevail to the extent of the conflict. Where the SCCs apply, any conflict will be resolved in favor of the SCCs with respect to the Processing of Personal Data.

If the Parties have negotiated and mutually executed another supplemental agreement governing the Processing of Personal Data under the Agreement, then that agreement applies in lieu of this DPA.

1. CONSTRUING THIS DPA.

- 1.1. This DPA must be interpreted as broadly as necessary to comply with Applicable Data Protection Law. This includes, where appropriate, applying to terms in this DPA their definitions given in Applicable Data Protection Law, including definitions for analogous terms. In case of any changes to Applicable Data Protection Law, then this DPA is deemed modified to conform with those changes. Customer has sole responsibility to notify Zasio if Customer believes that Personal Data provided to Zasio for Processing under the Agreement becomes subject to any privacy and security requirements from jurisdictions that are not incorporated into this DPA. If this happens, the Parties shall work in good faith to include the additional requirements in an amendment.
- 1.2. The following are attached and form part of this DPA:
 - Annex I:** List of Parties; Description of Transfer; and Competent Supervisory Authority
 - Annex II:** Technical and Organizational Measures
 - Annex III:** List of Sub-processors
- 1.3. **Term.** The term of this DPA coincides with the term of the Agreement. However, Zasio’s obligations with respect to the Processing of Personal Data will remain so long as Zasio Processes such Personal Data.
- 1.4. **Signature Requirements.** The Parties’ acceptance of this DPA satisfies all signature requirements under Applicable Data Protection Law.

2. DEFINITIONS.

“**Applicable Data Protection Law**” means all laws, regulations, and other legal requirements that apply to the Processing, protection, and privacy of Personal Data under the Agreement from: (i.) the European Union (“EU”) and European Economic Area (“EEA”), the United Kingdom (“UK”), and Switzerland (including all applicable European Data Protection Laws); (ii.) the United States (“US”); and (iii.) any other jurisdiction whose Personal Data protection laws are no more prescriptive than these laws.

“**Controller**” means the natural or legal person, Public Authority, agency, or other body which alone, or jointly with others, determines the purpose and means of Processing of Personal Data; or, where context requires, as defined under Applicable Data Protection Law.

“**Customer Data**” for this DPA means all data and information, regardless of form, submitted by or on behalf of Customer to Zasio to enable Zasio’s provision of Zasio Services to Customer, including Customer’s affiliates.

“**Data Subject**” means the identified or identifiable living individual to whom Personal Data relates; or, where context requires, as defined by Applicable Data Protection Law. Where the California Consumer Privacy Act (“CCPA”) applies, Data Subject means “Consumer” as defined in the CCPA.

“**European Data Protection Law**” means, individually, or collectively: (i) Regulation (EU) 2016/67 of the European Parliament and of the Council of 27 April 2016 (also known as the General Data Protection Regulation) (the “EU GDPR”); (ii) the EU GDPR as transposed into United Kingdom national law by operation of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications Amendments etc. (EU Exit) Regulations 2019 (the “UK GDPR”); and (iii) the Swiss Federal Act on Data Protection Act (the “FADP”); as well as all applicable laws which implement these laws.

“**Hosted Services**” for this DPA means Zasio Services provided to Customer in the form of a hosted application.

“**Information Security Incident**” for this DPA means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by Zasio and/or its Sub-processors.

“**Personal Data**” for this DPA means all Customer Data that Zasio Processes on behalf of Customer under the Agreement which relates to an identified or identifiable natural person; or where subject to Applicable Data Protection Law, such data constituting “personally identifiable information,” “personal information,” “personal data,” or any similar term, as defined under the Applicable Data Protection Law.

“**Processor**” means the entity which Processes Personal Data on behalf of the Controller; or, where context requires, as defined by Applicable Data Protection Law.

“**Process**” and “**Processing**” means any operations or set of operations performed upon Personal Data, or where context requires, as defined by Applicable Data Protection Law.

“**Standard Contractual Clauses**” (the “SCCs”) mean the unchanged standard contractual clauses, published by the European Commission, reference 2021/914, and which are incorporated by reference. Module 2 applies when Customer is acting as a Controller, and Module 3 applies when Customer is acting as a Processor. If new SCCs are approved and made available for data controller-to-data processor transfers, those new SCCs will be immediately applicable to this DPA, and will be incorporated by reference, replacing the existing SCCs.

“**Sub-processor**” means any Processor engaged to Process Personal Data by or on Zasio’s behalf under the Agreement; or, where context requires, as defined under Applicable Data Protection Law (including, as applicable, the definition for an analogous term). When Customer is acting as a Processor, Zasio is a Sub-processor.

“**Zasio Services**” means those services provided by Zasio to Customer as set forth in the Agreement, including its applicable order forms, statements of work, or similar written agreements with Zasio.

The terms “**Consumer**” “**Business Purpose**,” “**Business**,” “**Service Provider**,” “**Sell**,” and “**Share**” will be given their meanings in Applicable Data Protection Law, including where applicable the CCPA, and, where required, the meanings for analog terms under Applicable Data Protection Law.

3. PERSONAL DATA PROCESSING.

3.1 Roles & Obligations.

- a. Customer (including its users) is a Controller (or a Processor when acting on another Controller's behalf (e.g. Customer's affiliate)) and Zasio is a Processor (or, where the CCPA applies: Customer is a Business and Zasio is a Service Provider and Zasio shall comply with all obligations applicable to a Service Provider, including those related to Personal Data privacy and security).
- b. To the extent Zasio Processes Personal Data subject to European Data Protection Law for its business operations incident to providing Zasio Service to Customer, Zasio will comply with the obligations of an independent Controller.
- c. Customer shall disclose Personal Data to Zasio under the Agreement only for the limited purposes of providing Zasio Services in accordance with the Agreement.
- d. Zasio shall promptly notify Customer if Zasio determines it can no longer meet its obligations under this DPA.
- e. Customer shall use commercially reasonable efforts to minimize any transfer of Personal Data to Zasio to that appropriate to the Zasio Services Customer purchases under the Agreement.

3.2 Legal Compliance. Each Party shall comply with its respective obligations under Applicable Data Protection Law with respect to the Processing of Personal Data. Zasio does not, however, monitor Customer Data to determine whether any Customer Data includes information subject to any specific laws or regulations and, unless by separate written agreement, Zasio is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to Zasio.

3.3 Instructions. Zasio (including its Sub-processors) will Process Personal Data in compliance with Customer's lawful instructions and solely for the purpose of providing Zasio Services in accordance with the Agreement, unless required otherwise by Applicable Data Protection Law. Should Zasio have a legal obligation to Process Personal Data, Zasio shall notify Customer unless legally prohibited. The Agreement (including all of its order forms, SOWs, and exhibits and other appendices) describes Customer's complete instructions to Zasio regarding Zasio's Processing of Personal Data. Additional Processing beyond the scope of these instructions may only occur pursuant to the Parties' prior written agreement or to the extent required by Applicable Data Protection Law.

3.4 Combining Personal Data. Unless authorized under Applicable Data Protection Law and necessary to carry out Customer's instructions for Processing, Zasio shall not combine Personal Data with Personal Data it receives or collects from a third party.

3.5 Nature and Purpose of Processing. Annex I to this DPA sets out the Parties' agreed-upon subject matter, nature, and purpose of the Processing, type of Personal Data, and categories of Data Subjects. Where the SCCs apply, Annex I of this DPA constitutes Annex I of the SCCs.

3.6 Customer Responsibilities. Customer is responsible for the following with respect to its access and use of Zasio Services:

- a. Ensuring a level of security and configuration appropriate to the risk in respect of Personal Data Customer elects to store in Zasio Services; and
- b. Separately Backing up Personal Data that Customer elects to store in Zasio Services.

3.7 Data Location. Unless the Parties expressly agree otherwise in writing, Zasio will ensure all Personal Data provided to Zasio (including its Sub-processors) for Processing under the Agreement will be Processed in the United States.

3.8 Customer Obligations.

- a. **Accuracy, Quality, and Legality.** Customer is responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer has acquired and processes Personal Data.
- b. **Notices and Consents.** Customer shall provide all fair processing notices and obtain all consents, licenses, and legal bases required to allow Zasio to Process Personal Data under the Agreement. Zasio assumes no obligation to independently verify the adequacy or legality of the notices or consents or rights.

3.9 Additional Zasio Obligations.

- a. Zasio will not (i) Sell or Share (as those terms are defined under the CCPA, regardless of the CCPA's applicability) Personal Data; or (ii) disclose any Personal Data to a third party, except: (a.) to its Sub-processors to provide Zasio Services in accordance with the Agreement, or (b.) when required by applicable law.
- b. Zasio will also ensure that Zasio personnel authorized to Process Personal Data have committed to confidentiality requirements at least as protective as those in the Agreement (including this DPA).
- c. Unless contrary to Applicable Data Protection Law, Zasio will inform Customer if Zasio cannot comply with an instruction or, in Zasio's opinion, a Customer instruction violates Applicable Data Protection Law.

4. TECHNICAL AND ORGANIZATIONAL MEASURES.

- 4.1 **Appropriate Measures.** Zasio shall implement and maintain technical and organizational measures appropriate to its Processing of Personal Data and the risks of an Information Security Incident, taking into account the nature, scope, context, and purpose of the Processing, and the risks to the rights and freedoms of natural persons. Zasio's current measures are set forth in the document entitled Technical and Organizational Measures, which forms part of this DPA as Annex II. Where the SCCs apply, Annex II to this DPA constitutes Annex II to the SCCs.
- 4.2 **Customer's Determination.** Customer is responsible for making an independent determination of whether the Technical and Organizational Measures (i) are appropriate to Personal Data and Zasio Services; and (ii) meet Customer's requirements and security obligations with respect to Applicable Data Protection Law.
- 4.3 **Updates.** The Technical and Organizational Measures are subject to technical progress and development. Accordingly, Zasio may update these from time to time as long as any updates do not materially degrade Zasio's level of security. Zasio will publish any changes to the Technical and Organizational Measures by email, through its website, or through Zasio's Customer Service Portal, or by some or all of these means.

5. SUB-PROCESSORS.

- 5.1 **Engaging Sub-processors.** Zasio may engage Sub-processors to Process Personal Data under the Agreement; however, Zasio will not engage any Sub-processor without including contractual terms at least as protective as this DPA.
- 5.2 **Liability.** Zasio shall be liable for its Sub-processor's conduct to the extent that Zasio would be liable for the same conduct under the Agreement. This includes remaining responsible for compliance with the obligations of this DPA and any failure by a Sub-processor to fulfill its data protection obligations under Applicable Data Protection Law.

5.3 **Identity.** A list of Zasio’s Sub-processors relevant as of the Agreement Effective Date forms part of this DPA as Annex III. Customer consents to the Sub-processors included in this list. Where the SCCs apply, Annex III to this DPA constitutes Annex III of the SCCs.

5.4 **New Sub-processors.** Zasio may use new or replace existing Sub-processors to Process Personal Data, provided that Zasio gives Customer at least 30 days’ written notice before granting the Sub-processor access to Personal Data (a “**Review Period**”). Customer may in good faith object to a new Sub-processor during the Review Period, in which case Zasio shall use reasonable efforts to change Customer’s configuration or use of Zasio Services to avoid the Processing of Personal Data by the new Sub-processor. If Zasio is unable to fulfill such a requested accommodation within a commercially reasonable period, Customer may terminate the Agreement or the applicable Zasio Services, as applicable, by providing Zasio written notice if Customer has (i) a legitimate reason under Applicable Data Protection Law to object to the new Sub-processor; or (ii) legitimate concerns about the new Sub-processor with respect to the level of privacy and security of Personal Data required under the Agreement. Any termination under this Section 5.4 constitutes termination without cause; however, upon such termination Zasio will provide Customer a pro rata refund of any unused and prepaid fees for terminated Zasio Services. A lack of response by Customer during a Review Period constitutes Customer’s approval of the additional or replacement Sub-processors.

6. CROSS-BORDER TRANSFERS.

6.1. **SCCs.** To the extent Zasio Processes Personal Data subject to European Data Protection Law outside of a prescribed region without adequate alternative mechanism (as those terms are defined under European Data Protection Law) (a “**Restricted Transfer**”), each Party shall comply with the obligations set out in the SCCs, as completed in this DPA. Upon any conflict between this DPA and the SCCs, the SCCs will prevail to the extent of the conflict; however, each Party’s aggregate liability under this DPA will not exceed the Agreement’s liability caps and limitations.

6.2. Completing the SCCs.

a. Where the EU GDPR applies to a Restricted Transfer, the SCCs are completed as follows:

- i. In Clause 7, the optional docking clause will apply;
- ii. For Clause 9, Option 2 will apply and will be completed and subject to Section 5 (SUB-PROCESSORS) of this DPA;
- iii. The optional redress language in Clause 11 will not apply;
- iv. For Clause 17, Option 2 will apply, and the SCCs will be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.
- v. For Clause 18(b), the Parties agree that the courts will be the Netherlands;

b. Where the UK GDPR applies to a Restricted Transfer, the UK IDTA (the International Data Transfer Addendum to the SCCs, issued by the UK Information Commissioner under Section 119A(1) Data Protection Act 2018, as may be amended, or superseded from time to time by the UK government) will apply, and is completed as follows:

- i. **Table 1:** The start date is the effective date of the Agreement; the Exporter is Customer, and the Importer is Zasio; the Importer’s and Exporter’s details and contact information are found in Annex I to this DPA.

- c. Customer has a direct audit right under Applicable Data Protection Law; or
- d. Customer reasonably believes that the information provided pursuant to DPA Sections 7.1 and 7.2 is insufficient to demonstrate Zasio's compliance with the Security Requirements.

7.4 **Audit Costs.** Customer must bear the costs of any audit unless doing so would be contrary to Applicable Data Protection Law. Zasio will promptly remedy at its own cost any breach discovered as a result of an audit.

7.5 **Conditions.** Unless Applicable Data Protection Law requires otherwise, any audit under DPA Section 7.3 will only be (i) upon reasonable advance notice; (ii) during normal business hours; (iii) subject to Zasio's reasonable security and confidentiality requirements; and (iv) carried out no more than once every 12 months (unless performed in response to an Information Security Incident).

7.6 **Legal Compliance.** In addition to the above Section 7 provisions, and where required of Zasio under Applicable Data Protection Law, Zasio will make available to Customer all information in its possession that is reasonably necessary to demonstrate Zasio's compliance with its obligations under Applicable Data Protection Law, including allowing and cooperating with reasonable inspections or audits as required or permitted under applicable Data Protection Law.

8. DATA PROTECTION IMPACT ASSESSMENTS.

Taking into account the nature of the Personal Data Processing and information available to Zasio, and at Customer's request and reasonable expense, Zasio shall provide Customer with reasonably requested information regarding Zasio Services to assist Customer in carrying out any data protection impact assessment (or analogous task) required under Applicable Data Protection Law.

9. ACCESS AND PROCESSING REQUESTS.

9.1. **Data Subject Requests.** Zasio shall promptly (i.) forward to Customer any request received from a Data Subject seeking to exercise their rights under Applicable Data Protection Law, and (ii.) inform the Data Subject of the same. Customer has primary access rights to Personal Data stored using the Hosted Services and is solely responsible for responding to such a request, unless contrary to Applicable Data Protection Law. To the extent that Customer is unable to independently access relevant Personal Data, Zasio shall, upon Customer's request, reasonably assist Customer, and where legally permitted, at Customer's reasonable expense, to enable Customer to respond to:

- a. A Data Subject seeking to exercise their rights under Applicable Data Protection Law; and
- b. Correspondence, inquiry, or complaint received from a Public Authority, regulator, or third-party in connection with Zasio's Processing of Personal Data.

Unless contrary to Applicable Data Protection Law, Zasio will not respond to any request made directly to Zasio without Customer's authorization, unless the response is to inform the requestor that Zasio lacks authority to respond directly and recommend the request be sent directly to Customer. Customer shall communicate to Zasio all Data Subject requests with respect to Personal Data, and where applicable, ensure it maintains a record of consent to processing for each Consumer.

Customer is solely responsible for ensuring Data Subject requests for erasure, restriction, or cessation of processing, or withdrawal of consent to processing, are communicated to Zasio where necessary for Zasio to help fulfill the request.

9.2. **Public Authority Requests.** If a Public Authority (defined to mean law enforcement, regulatory agency, or supervisory authority) provides Zasio a demand for Personal Data (including via a subpoena or court order), Zasio will attempt to redirect the Public Authority to Customer (including providing the Public Authority with Customer's contact information). If Zasio is compelled to disclose Personal Data to a Public Authority, Zasio

shall, to the extent legally permitted, give Customer reasonable notice and allow Customer to seek an appropriate remedy, such as a protective order.

9.3. Request Notice. If Zasio is legally required to respond to a request under this Section 9, Zasio will promptly notify Customer and provide it with a copy unless legally prohibited.

10. INCIDENT NOTIFICATION.

10.1 Notice to Customer. If Zasio becomes aware of an Information Security Incident, Zasio will notify Customer without undue delay (where feasible, no later than 72 hours after discovery) and in accordance with applicable law. Zasio will promptly investigate the cause, take steps to mitigate the impact, and work to prevent a recurrence. As information becomes available, Zasio will promptly inform Customer of: (i) the nature and reasonably anticipated consequences of the Information Security Incident; (ii) mitigation steps taken and efforts to prevent a recurrence; (iii) where possible, the types of Personal affected; and (iv) any other information required by applicable law. Zasio’s actions under this Section do not constitute an admission of fault or liability.

11. GOVERNING LAW.

Unless Applicable Data Protection Law requires otherwise, this DPA will be governed in accordance with the governing law and jurisdiction requirements of the Agreement. If no such requirements are stated, then the laws of the State of Idaho will apply, excluding its conflicts of law provisions, and the jurisdiction to resolve any dispute will be the state and federal courts located in Ada County, Idaho.

12. PERSONAL DATA DELETION.

Upon the Agreement’s termination, Zasio shall delete or return any Personal Data (i) consistent with the terms of the Agreement and Applicable Data Protection Law; and (ii) as soon as reasonably practicable; unless applicable law requires further storage. If Customer does not provide Zasio with any return or deletion instructions, then Zasio will retain and destroy Personal Data in the normal course pursuant to its standard retention and destruction policies.

EXECUTED BY THE PARTIES’ AUTHORIZED REPRESENTATIVES.

| | |
|---------------------------------|---|
| ZASIO ENTERPRISES, INC.: | [Insert Customer Full Legal Name]: |
| By: | By: |
| Name: | Name: |
| Title: | Title: |
| Date: | Date: |

ANNEX I

This Annex I establishes the agreed subject-matter, the nature and purpose of Processing, the type of Personal Data, and the categories of Data Subjects in respect of Zasio's Processing of Personal Data under the Agreement. This Annex I shall also serve as Annex I of the SCCs, where applicable.

A. LIST OF PARTIES.

i. Data exporter(s):

Name: Customer and its users, as identified in the Agreement.

Address: Customer's address, as identified in the Agreement.

Contact person's name, position and contact details: As identified in the Agreement.

Activities relevant to the data transferred under these Clauses:

Performance of Zasio Services pursuant to the Agreement. And specifically:

For On-Premises Software: Support and Professional Services.

For Hosted Services: Hosted Services, Support and Professional Services.

For Consulting Services: Consulting Services.

Signature and date: These SCCs shall be deemed executed by Customer upon the effective date of the Agreement

Role (controller/processor): Controller and/or Processor.

ii. Data importer(s):

Name: Zasio Enterprises, Inc.

Address: 401 W. Front St., Ste. 305, Boise, ID 83702

Contact person's name, position and contact details: Cindy Zasio, Vice President of Operations, cindy.zasio@zasio.com

Activities relevant to the data transferred under these Clauses:

Performance of Zasio Services pursuant to the Agreement. And specifically:

For On-Premises Software: Support and Professional Services.

For Hosted Services: Hosted Services, Support and Professional Services.

For Consulting Services: Consulting Services.

Signature and date: These SCCs shall be deemed executed by Zasio upon the effective date of the Agreement.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER.

i. Categories of Data Subjects whose personal data is transferred:

- i. Customer's, including authorized affiliates', users, employees, contractors, and agents, as permitted under the Agreement.
- ii. Customer controls the categories of Data Subjects it shares with Zasio and when it shares this information in support of Zasio's provision of Zasio Services, as well as maintaining Customer's account with Zasio, pursuant to the Agreement.

ii. Categories of Personal Data transferred:

- i. Identification and contact data (such as name, address, title, contact details), employment details (like job title, role, manager), and/or IT information (e.g., IP addresses, including IP derived geolocation), activity data (including access request activity, authentication activity, and provisioning activity).
- ii. Customer controls information it shares with Zasio and when it shares this information in support of Zasio's provision of Zasio Services, as well as maintaining Customer's account with Zasio, pursuant to the Agreement.

iii. Sensitive data transferred (if applicable) and applied restrictions or safeguards:

Not Applicable: Zasio Services are not intended for the Processing of sensitive Personal Data.

iv. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

On a continuous basis, the frequency of which is determined by Customer. Customer controls what information it shares with Zasio and when it shares this information in support of Zasio's provision of Zasio Services, as well as maintaining Customer's account with Zasio, pursuant to the Agreement.

v. Nature of the processing:

Personal Data processing activities include the storage and management of Personal Data to allow Zasio and its Sub-processors to provide Zasio Services as described in the Agreement.

vi. Purpose(s) of the data transfer and further processing:

Customer will transfer Personal Data to Zasio for Processing by Zasio as necessary to provide Zasio Services to Customer.

vii. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

For the duration of Processing by Zasio in connection with the provision of Zasio Services under the Agreement, and thereafter as outlined in the Agreement and to comply with applicable law, including Applicable Data Protection Laws. Zasio is not required to delete or return Personal Data to the extent: (i) Zasio is required to retain the Personal Data by applicable law or government or regulatory order; and/or (ii) the Personal Data is archived on back-up or recovery systems, which Personal Data Zasio will securely isolate and protect from further processing, except where required otherwise by applicable law.

viii. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

The nature and purposes of the Processing by Sub-processors is the provision of Zasio Services to Customer, as provided for in the Agreement; the duration is until the termination of Zasio Services to which the Personal Data relates.

C. COMPETENT SUPERVISORY AUTHORITY.

The competent supervisory authority shall be determined in accordance with Clause 13 of the SCCs.

ANNEX II
TECHNICAL AND ORGANIZATIONAL MEASURES

Zasio's current technical and organizational measures are described [here](#).

ANNEX III
LIST OF SUBPROCESSORS

Zasio's list of current Sub-processors is contained [here](#).