# Data Protection Addendum

This Data Protection Addendum (**"DPA"**) is entered into between Coalition, Inc. and its Affiliates (**"Coalition**" defined below, also referred to as **"Processor"**) and Client (defined below, also referred to as **"Controller"**, or may be referred to as **"Customer"** in the Agreement). Coalition and Client shall each be referred to as a **"Party"** and collectively as the **"Parties"**. This DPA is effective as of the effective date of the Agreement (**"Effective Date"**).

## I. Applicability and Effective Date

This DPA is made pursuant to Applicable Privacy Laws (defined below) including but not limited to CCPA (defined below) and GDPR (defined below). This DPA shall amend and be incorporated into any current valid written contracts between the Parties requiring the processing of Personal Data on behalf of Controller by Processor (collectively, the **"Agreement"**).

## II. Definitions

Capitalized terms not otherwise defined herein shall have the meaning given to them under the Agreement or Applicable Privacy Law. In particular, the terms **"Commission"**, **"Controller"**, **"Personal Data Breach"**, **"Processor"** and **"Supervisory Authority"** shall have the meaning as set forth in the GDPR. The terms **"Data Exporter"** and **"Data Importer"** shall have the same meaning as in the Standard Contractual Clauses. The terms **"Business"**, **"Business Purpose"**, **"Collects"**, **"Consumer"**, **"Contractor"**, **"Person"**, **"Processing"**, **"Sell"**, **"Service Provider"**, and **"Share"** shall have the meaning set forth in the CCPA. The following terms in the GDPR and CCPA are understood to have the same meaning: **"Controller"** and **"Business"**, **"Data Subject"** and **"Consumer"**, **"Processor"** and **"Service Provider"**, and **"Person"** and **"Subprocessor"**.

**"Affiliates"** means any company that controls, is controlled by, or is under common control with another company.

**"Applicable Privacy Laws"** means any laws that regulate the Processing, privacy or security of Client Personal Data and that are directly applicable to each Party when Processing Client Personal Data. Applicable Privacy Laws include but are not limited to (i) the General Data Protection Regulation (EU) 2016/679 (**"GDPR"**) and any local laws implementing or supplementing the GDPR, (ii) the United Kingdom (**"UK"**) Data Protection Act 2018 and the 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 (**"UK GDPR"**), (iii) the California Consumer Privacy Act of 2018 effective January 1, 2020, and its implementing regulations, as amended or superseded from time to time (**"CCPA"**), (iv) the Australia Privacy Act 1988 (No. 119 1988), as amended (**"Privacy Act"**), and the Australian Privacy Principles (**"APPs"**), (v)

Canadian Personal Information Protection and Electronic Documents Act (**"PIPEDA"**) and substantially similar provincial laws, and (vi) Swiss Data Protection Laws.

**"Client"** means the person or entity that has entered into the Agreement with Coalition.

**"Client Personal Data"** means (i) Personal Data as defined under GDPR, (ii) Personal Information, as defined under CCPA, and/or (iii) similar terms as defined under Applicable Privacy Laws processed by Processor, or its Subprocessor (as applicable), on behalf of Client in the provision of the Services pursuant to the Agreement.

**"Coalition"** means Coalition, Inc. or the Affiliate of Coalition, Inc. that entered into the Agreement with Client. Coalition entities are listed in Exhibit 3 to this DPA.

**"Data Subject"** means (i) "data subject" as defined under GDPR, (ii) "consumer" as defined under CCPA, or (iii) similar term under Applicable Privacy Laws.

**"EEA"** means the member states of the European Union and Iceland, Liechtenstein and Norway.

**"EEA SCCs"** means Module 2 (Controller to Processor) of the Standard Contractual Clauses for the transfer of personal data to Third Countries set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (and "EEA SCCs" shall be construed accordingly), specifically:

a) the optional docking clause 7 of the EEA SCCs does not apply and is deemed to be deleted;

b) for the purposes of clause 9 of the EEA C2P SCCs, option 2 (General Written Authorisation) applies and the relevant time period is 15 calendar days;

c) the independent dispute resolution option in clause 11 of the EEA SCCs does not apply;

d) for the purposes of clause 17 of the EEA SCCs, the chosen option is option 1 and the chosen law is that set forth under the Agreement. If none provided, the chosen law shall be that of Ireland;

e) for the purposes of clause 18(b) of the EEA SSCs, the chosen courts are courts set forth under the Agreement. If none provided, the chosen courts are those in Ireland;

f) the Appendices of the EEA SCCs shall be completed as follows:

1. Client shall be the controller and data exporter and Coalition shall be the processor and data importer for the purposes of Annex I.A to the EEA SCCs and the contact information for each shall be as follows:

(i) Client contact person's name, position and contact details: as forth in the Agreement; and

(ii) Coalition contact person's name, position and contact details: as set forth in the Agreement.

2. the contents of Exhibit 1 shall form Annex I.B to the EEA SCCs;
3. the competent supervisory authority shall be Ireland for the purposes of Annex I.C to the EEA SCCs;
4. the contents of Exhibit 2 shall form Annex II to the EEA SCCs; and
5. the contents of Exhibit 4 shall form Annex III to the EEA SCCs.

**"Restricted Transfer"** means any transfer of Client Personal Data by Client to Coalition in a Third Country where (1) the transferring Client entity is established in the UK, EEA or Switzerland and/or (2) the Personal Data originated in the UK, the EEA or Switzerland.

"**Sensitive Data**" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) financial or credit information, credit or debit card number; (c) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sex life or sexual orientation, or data relating to criminal convictions and offences; (d) Personal Data relating to children; and/or (e) account passwords in unhashed form.

**"Services"** means any and all services or subscriptions provided by Coalition to Client pursuant to the Agreement.

**"Standard Contractual Clauses"** means the applicable module of the EEA, the Swiss or the UK government-approved contract mechanism for the cross-border transfer of Client Personal Data from the EEA, Switzerland or the UK (as applicable) to Third Countries.

**"Swiss SCCs"** means the EEA SCCs, as amended as follows:

a) general and specific references in the EEA SCCs to Regulation (EU) 2016/679 or "that Regulation" or EU or member state law have the same meaning as the equivalent reference in Swiss Data Protection Law;

b) the term "member state" will not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with clause 18(c) of the EEA SCCs;

c) the details of the transfers are those specified in Schedule 1 where Swiss Data Protection Law apply to the transfer;

d) the EEA SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as "Personal Data" under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity; and

e) the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for the purposes of clause 13 of the EEA SCCs.

**"Swiss Data Protection Law"** means the data protection and privacy laws and regulations of Switzerland.

**"Third Countries"** means countries other than (1) EEA member states; (2) Switzerland; (3) the UK or (4) those subject to an adequacy Client Personal Data by the European Commission and/or the UK Secretary of State (as applicable) from time-to-time.

**"UK Addendum"** means the International Data Transfer Addendum issued by the Information Commissioners' Office under s.119(A) of the UK Data Protection Act 2018 as may be updated from time-to-time, currently found at International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

**"UK SCCs"** means the UK Addendum, where:

a) Table 1 and Table 3 of the UK Addendum are deemed to have been completed with the corresponding details set out in Exhibit 1 to this DPA and, for the purposes of Table 1 of the UK Addendum,

1. the "Start Date" is the Effective Date; and
1. the official company registration numbers (where applicable) of the Parties are as set out in the Agreement;

b) for the purposes of Table 2 of the UK Addendum, (1) the version of the "Approved EU SCCs" is the EEA SCCs; (2) the choices regarding clause 7 (docking clauses), clause 11 (option), clause 9a (prior authorisation or general authorisation) and clause 9a (time period) of the EEA SCCs are as set out in the definition of EEA SCCs in this DPA; and

c) "Importer" is deemed to have been chosen for the purposes of Table 4 of the UK Addendum.

## III. Processing of Client Personal Data

A. Processor shall only Process Client Personal Data on behalf of Controller in accordance with this DPA and in accordance with Controller's instructions, unless Processing is required by Applicable Privacy Laws to which Processor is subject, in which case Processor shall, to the extent permitted by Applicable Privacy Law, inform and coordinate with Controller prior to Processing.

B. Processor acknowledges and agrees that Exhibit 1 (Description of Processing Activities) to this DPA is an accurate description of the Processing carried out under this DPA, which shall be amended from time to time to reflect accurate nature, duration, purpose, types and categories related to the Processing of Client Personal Data. The Parties agree that the Services are not intended for the Processing of Sensitive Data, and that if Controller wishes to use Services that include Wizer to Process Sensitive Data, it must first obtain Wizer's explicit prior written consent and enter into any additional agreements as may be required by Wizer, if applicable and necessary as governed by the particular platform of Coalition that is used by Controller under the Services.

C. Processor shall not sell or disclose Client Personal Data to third parties other than as provided under this DPA. No copies or duplicates of Client Personal Data may be produced without the knowledge of Controller. This does not apply to the creation of backup copies to facilitate compliance with Applicable Privacy Laws.

D. To the extent required by Applicable Privacy Laws, Processor shall maintain a record of all categories of Processing activities carried out on behalf of Controller, which shall be compliant with Applicable Privacy Laws.

E. The Parties agree that Processor may reproduce and use data in a de-identified, aggregated, and generic manner ("**De-Identified Data**") for the purpose of: (i) maintenance, support, and development of its Service; (ii) tracking subscriber's Service usage statistics and metrics; (iii) reporting and analyzing threat intelligence; or (iv) other similar purposes. Processor may also publish or share De-Identified Data to conduct or facilitate academic research or to release marketing or statistical data. If Processor disclose or publish any De-Identified Data, it will only be in a generic or aggregated form that will not identify the Client Personal Data or any individuals, or Client Confidential Information (as defined in the Agreement). The Processor shall de-identify data in accordance with Applicable Privacy Laws and implement industry-standard technical safeguards to prevent reidentification of data to prevent inadvertent release of Client Personal Data or Confidential information.

## IV. Notification Obligations

A. Processor shall immediately notify Controller of any monitoring activities and measures undertaken by a supervisory authority or other applicable regulatory body in respect of it, to the extent such monitoring activities and measures are made in connection with Client Personal Data.

B. Processor shall immediately and in any event within 5 business days inform the Controller in the event that it receives a request from a Data Subject relating to the Client Personal Data.

C. Processor shall notify Controller of a Personal Data Breach without undue delay of Processor becoming aware of the Personal Data Breach. In consultation with Controller, Processor shall take reasonable and appropriate measures in accordance with Applicable Privacy Laws and industry standards to secure Personal Data and limit possible detrimental effects to Data Subjects. Where obligations are placed on Controller under Applicable Privacy Laws, Processor must provide reasonable assistance to Controller in meeting such obligations.

## V. Technical and Organizational Measures

Processor shall implement the technical and organizational measures set forth in Exhibit 2 (Technical and Organizational Measures). Processor shall maintain appropriate industry-standard technical and organizational measures for protection of Client Personal Data Processed hereunder (including measures against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Personal Data, confidentiality, and integrity of Client Personal Data).

## VI. Authorized Persons and Training

Processor shall ensure that only its designated authorized persons shall be provided access to Client's Personal Data. Processor shall ensure that its designated authorized persons receive adequate training to ensure compliance with Processing requirements under this DPA and are subject to a confidentiality agreement or are under an appropriate statutory obligation of confidentiality.

## VII. Compliance with Applicable Privacy Laws

Upon written reasonable request of Controller and taking into account the nature of Processing and information available, Processor shall assist Controller, at Controller's cost, in ensuring compliance with the obligations pursuant to Applicable Privacy Laws, including but not limited to security of Processing, Personal Data Breach notification, data protection impact assessment, consultation with or requests of a competent data protection authority and inquiries about Controller's Processing of Client Personal Data pursuant to this DPA. To the extent required and permitted under Applicable Privacy Laws Processor shall provide all available information to Controller to demonstrate compliance with personal data processing obligations under this DPA.

## VIII. Data Protection Officer

Where stipulated by Applicable Privacy Laws, Processor shall appoint a data protection officer ("DPO") to fulfill the duties and responsibilities set forth under Applicable Privacy Laws. Processor has appointed a DPO that may be reached at privacy@coalitioninc.com.

## IX. Audit Rights of Controller

Upon Controller's prior written request at reasonable intervals (but no more than once every 12 months, with the exception of a Personal Data Breach by Processor, and in such event Controller may request an audit despite the current audit interval), and subject to strict confidentiality undertakings by Controller, Processor shall make available to Controller that is not a competitor of Processor (or Controller's independent, reputable, third-party auditor that is not a competitor of Processor and not in conflict with Processor, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them. Processor may satisfy its obligations under this section by answering Controller's questionnaire-based audits and/or by providing Controller with attestations, certifications and summaries of audit reports conducted by accredited third party auditors solely related to Processor's compliance with this DPA. Any information relating to audits, inspections, and the results therefrom, including the documents reflecting the outcome thereof, shall only be used by Controller to assess Processor's compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Processor's prior written approval. Upon Processor's first request, Controller shall transfer to Processor all records or documentation that was provided by Processor or collected and/or generated by Controller (or each of its mandated auditors) in the context of the audit and/or the inspection.

## X. Data Subject Rights

Taking into consideration the nature of Client Personal Data Processing, Processor shall:

1. Not respond to the Data Subject request itself or by Subprocessor unless required by Applicable Privacy Laws.

2. Notify Controller without undue delay if Processor or any Subprocessor receives a request from a Data Subject under any Applicable Privacy Laws with respect to Client Personal Data.

3. Reasonably assist Controller through appropriate technical and organizational measures to fulfill Controller's obligation to respond to Data Subject requests arising under Applicable Privacy Laws.

## XI. Deletion of Client Personal Data

A. Processing of Client Personal Data by Processor shall only take place for the duration specified in the Agreement, unless terminated earlier pursuant to the terms and conditions of the Agreement ("**Processing Time Frame**"); provided however, and if applicable,Processor preserves user data associated with a terminated or expired Wizer account for a period of ninety (90) days following the termination or expiration of such account subscription. In specific circumstances, Wizer may prolong the retention of certain user data when it is necessary: (i) by legal, regulatory, tax, or accounting requirements, (ii) for maintaining an accurate record of the user interactions with Wizer in case of complaints or challenges, if applicable; or (iii) if applicable, Wizer reasonably believes there is a potential for litigation related to such user data.

B. Subject to the above said, at the end of the Processing Time Frame:

1. Client Personal Data will be deleted within ninety (90) days following the end of the Processing Time Frame, unless retention of Client Personal Data is required pursuant to Applicable Privacy Laws or the circumstances described above.
2. Upon Controller's written request, Processor shall, at the choice of Controller:
    a. Return the Client Personal Data to Controller; or
    b. Delete the Client Personal Data and provide Controller with a written confirmation of deletion of the Client Personal Data.

## XII. Subprocessors

A. Processor may engage Subprocessors to assist in providing the Services to the extent permitted under this Section XII. Processor shall maintain a list of Subprocessors that process Client Personal Data and shall provide a copy of such list to Controller upon request. As of the Effective Date, Controller hereby grants Processor general written authorization to engage with the Sub-processors set out at Exhibit 4 hereto, which are currently used by Processor to process Personal Data.

B. Processor shall carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Client Personal Data required by Applicable Privacy Laws, this DPA and the Agreement. Processor shall enter into a written agreement with each Subprocessor, to the extent applicable to the nature of the Services provided by such Subprocessor. Processor shall maintain copies of its agreements with Subprocessors and make such agreements available as Controller may request from time to time. To the extent necessary to protect confidential information, Processor may redact copies prior to sharing with Controller.

C. To the extent a Subprocessor is established in a Third Country, Processor shall ensure that any onward transfer of Personal Data originally transferred pursuant to clause XIII(A) shall be made in compliance with the requirements of the Applicable Privacy Law and in particular, where required, that Processor (as data exporter) and the Subprocessor (as data importer) will enter into the applicable Standard Contractual Clauses.

A. Processor shall be liable for the acts and omissions of its Subprocessors to the same extent Processor would be liable if performing the Services under the terms of this DPA.

E. Processor shall provide Controller with written notice of newly appointed Subprocessors (including the jurisdiction in which each Subprocessor is established) before authorizing such Subprocessors to Process Client Personal Data in connection with providing the Services. Controller may object to Processor's appointment of a new Subprocessor by providing written notice to Processor within fifteen (15) calendar days of receiving Processor's notification. Such notice shall explain the reasonable grounds for the objection. In the event Controller objects to a new Subprocessor, Processor will use commercially reasonable efforts to make available to Controller a change in the Services or recommend a commercially reasonable change to Controller's configuration or use of the Services to avoid the Processing of Client Personal Data by the objected-to new Subprocessor without unreasonably burdening Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) calendar days, either Party may terminate this DPA without penalty by providing written notice to the other Party.

## XIII. Restricted Transfers

A. To the extent that a Restricted Transfer of Client Personal Data is made:

1. To the extent that the Client Personal Data originated in the EEA and/or the Controller is established in the EEA, the EEA SCCs shall apply;
2. To the extent that the Client Personal Data originated in Switzerland and/or the Controller is established in Switzerland, the Swiss SCCs shall apply; and/or
3. To the extent that the Client Personal Data originated in the UK and/or the Controller is established in the UK, the UK SCCs shall apply.

B. Where Clause XIII(A) of this DPA applies, the Parties agree to be bound by, observe, comply with and perform the applicable Standard Contractual Clauses as if the Standard Contractual Clauses were set out in, and incorporated into this DPA. Controller and Processor are deemed to have executed and signed the applicable Standard Contractual Clauses by entering into this DPA.

## XIV. General Terms

A. **Governing Law and Jurisdiction**. The Parties to this DPA hereby submit to the choice of jurisdiction specified in the Agreement.

B. **Order of Precedence**. In the event of any inconsistency between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail solely with respect to the Processing of Client's Personal Data. The EEA SCCs, UK SCCs and/or Swiss SCCs (as applicable) shall take precedence over the provisions of this DPA and the Agreement solely with respect to the Processing of Client's Personal Data.

C. **Changes in Applicable Privacy Laws**. In the event of any changes to Applicable Privacy Laws affecting the terms of this DPA, the Parties agree to negotiate in good faith the amendment of this DPA as applicable and necessary to comply with the changes in Applicable Privacy Laws.

D. **Severance**. Should any provision of this DPA be deemed invalid or unenforceable by a court of competent jurisdiction, then the remainder of this DPA shall remain in full force and effect. The invalid or unenforceable provisions shall either be: (a) amended by the Parties as necessary to ensure validity and enforceability, while preserving the Parties' intentions as closely as possible; or, if (a) is not feasible, construe such provision in a manner as if the invalid or unenforceable provision was not originally made a part of this DPA.

E. **Assignment of Rights and Delegation of Duties**. Any assignment of rights or obligation hereunder by a Party hereto shall be made in accordance with the Agreement.

F. **Force Majeure.** Non-performance of either Party will be excused to the extent performance is rendered impossible by strike, fire, war, flood, governmental acts or orders or restrictions, or act of God, or any other reason where failure to perform is beyond the reasonable control of the non-performing Party.

G. **Nature of DPA**. Nothing in this DPA shall be construed to create (i) a partnership, joint venture or other joint business relationship between the Parties or any of their affiliates, (ii) any fiduciary duty owed by one Party to another Party or any of its affiliates, or (iii) a relationship of employer and employee between the Parties.

H. **No Waiver**. Failure or delay on the part of either Party to exercise any right, power, privilege, or remedy hereunder shall not constitute a waiver thereof. No provision of this DPA may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.

I. **No Third Party Beneficiaries**. Save as otherwise provided by the EEA SCCs, UK SCCs and/or Swiss SCCs (as applicable) nothing in this DPA shall be considered or construed as conferring any right or benefit on a person not Party to this DPA nor imposing any obligations on either Party hereto to persons not a Party to this DPA.

J. **Term**. The term of this DPA shall commence on the Effective Date and terminate concomitantly with the Agreement, unless terminated earlier in accordance with this Section XIV.

K. **Termination.** Either Party may terminate this DPA immediately if the non-breaching Party determines, in its sole and reasonable discretion, that the other Party has breached a material term of this DPA and a cure is infeasible. Otherwise, the non-breaching Party shall provide the breaching Party with thirty (30) days from the breaching Party's receipt of a notice to cure such breach. If the breaching Party fails to cure such breach within thirty (30) days, then the non-breaching Party may terminate this DPA.

L. **Entire Agreement**. The Parties acknowledge and agree that they have read, understood and accept this DPA, including any exhibits and attachments, and that this DPA constitutes the entire agreement between them as to the subject matter herein, and supersedes all other communications, written or oral, relating to the subject matter of this DPA.

# Exhibit 1 - Description of Processing Activities

**Nature and Purpose of Processing**

1. Providing Services stipulated in the Agreement and/or other contracts executed by and between the Parties to Client.
2. Performing the Agreement, this DPA and/or other contracts executed by and between the Parties.
3. Acting upon Client's instructions, where such instructions are consistent with the terms of the Agreement.
4. Sharing Client's Personal Data with third parties in accordance with Client's instructions and/or pursuant to Client's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Client to facilitate the sharing of Client Personal Data between the Services and such third-party services).
5. Rendering Client Personal Data to be De-Identified Data.
6. Complying with applicable laws and regulations.
7. All tasks related to any of the above.

**Duration of Processing**

Subject to any section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Processor will Process Client's Personal Data for the duration of the Agreement and provision of the Services thereunder, unless otherwise agreed upon in writing; provided however that Vendor preserves user data associated with a terminated or expired Wizer account for a period of ninety (90) days following the termination or expiration of such account subscription (if use of Wizer is applicable to the specific Processor platform used by Controller). In specific circumstances, Processor may prolong the retention of certain user data when it is necessary: (i) by legal, regulatory, tax, or accounting requirements, (ii) for maintaining an accurate record of the user interactions with Wizer in case of complaints or challenges (if applicable), or (iii) if Wizer reasonably believes there is a potential for litigation related to such user data (if applicable).

**Type of Personal Data**

Subject to the provisions of the Agreement and this DPA, Controller may submit Personal Data to the Services, the type and extent of which is determined and controlled by Controller in its sole discretion. The Parties agree that the Services are not intended for the Processing of Sensitive Data, and that if Client wishes to use the Services to Process Sensitive Data, it must first obtain Wizer's explicit prior written consent and enter into any additional agreements as may be required by Wizer, if Wizer is applicable to the specific platform used by Controller.

**Categories of Data Subjects**

The Categories of Data Subjects relating to the Client Personal Data that will be processed by Processor are dependent on Controller, and may include, but are not limited to, any of the following categories:

- Employees, agents, advisors, freelancers of Client (who are natural persons).
- Prospects, customers, business partners and vendors of Client (who are natural persons).
- Any other third-party individual whose Personal Data is Processed by the Services.

# Exhibit 2 - Technical and Organizational Measures

## 1. General Considerations

This Exhibit 2 outlines the technical and organizational measures ("TOMs") Processor shall implement and maintain for secure and compliant processing of personal data. TOMs shall take into account the rights of data subjects and requirements of Applicable Privacy Laws, such as Articles 24, 25 and 32 GDPR to the extent applicable.

## 2. Organization

If required under Applicable Privacy Laws, Processor shall appoint a data protection officer (DPO) who shall provide advice on data privacy issues, update Processor about changes in Applicable Data Privacy Laws and support the review and improvement of these TOMs.

## 3. Confidentiality

### *3.1 Entry Control*

Processor shall maintain and enforce a physical security policy which governs physical security controls for both remote work and office requirements.

### *3.2 Access and Usage Control*

Processor shall restrict access to authorized users for all personal data and implement automatic control mechanisms for verifying access to systems containing personal data. User access to personal data shall be reviewed by Processor on an annual basis. Processor shall maintain strict password policies, including two factor authentication, for any application storing personal data. Access shall be monitored and logged, including unsuccessful login attempts. The use of personal data shall be limited, so that only authorized individuals can use the personal data necessary for their task (De Minimum Principle).

## 4. Integrity and Availability

Processor shall maintain sufficient and appropriate (based on the type of personal data exported and its sensitivity) environmental, physical and logical security measures with respect to personal data and to Processor's system infrastructure. This includes but is not limited to the following:

- Require all devices with access to personal data to meet industry security standards, including the installation of anti-malware software.
- Encryption of personal data based on data classification, both in transit and at rest.
- Personal data is processed on data processing systems that are subject to regular and documented patch management.

- Require redundant storage media and backups of systems according to latest technical standards.
- Conduct risk assessments and penetration testing on an annual basis to identify vulnerabilities, with remediation of such vulnerabilities.
- Security monitoring of systems and facilities storing personal data.
- Abide by established document retention and destruction policies for all personal data.
- Maintain an inventory of personal data with disposal instructions.
- Regular auditing of data processing procedures.
- Implementation and maintenance of procedures regarding data breaches and the protection of data subjects' rights.
- Regular review of technical advancements.

**5. Privacy-by-Default**

Processor shall incorporate privacy-by-design principles for systems and enhancements at the earliest stage of development.

**6. Employee Workplace**

Processor shall require its employees to complete privacy and security trainings on an annual basis.

# Exhibit 3 - Coalition Entities

| Entity Name | Country of Establishment | Registered Number | Registered Address | Contact Point for Data Protection Inquiries |
|---|---|---|---|---|
| Coalition, Inc. | United States of America | 820756527 (DE) | Paracorp Incorporated<br>2140 S. Dupont Highway<br>Camden, DE 19934 | privacy@coalitioninc.com |
| Coalition Insurance Solutions, Inc. | United States of America | 4018528 (CA) | 55 2nd Street, Suite 2500<br>San Francisco, CA 94105 | privacy@coalitioninc.com |
| Coalition Incident Response, Inc. | United States of America | 8340378393 (DE) | Paracorp Incorporated<br>2140 S. Dupont Highway<br>Camden, DE 19934 | privacy@coalitioninc.com |
| Coalition Risk Solutions Ltd. | United Kingdom | 13036309 | 34-36 Lime<br>Street London EC3M 7AT,<br>United Kingdom | privacy@coalitioninc.com |
| BinaryEdge, AG | Switzerland | CHE-376.026.878 | Witelellikerweg 10<br>CH-8702 Zollikon (CH) | privacy@coalitioninc.com |
| COALITION - Deiniram Soluções de Segurança, Unipessoal, Lda. | Portugal | 516582720 | Rua<br>Alexandre<br>Herculano, 38 – 4, 1250-011<br>Lisboa | privacy@coalitioninc.com |
| Coalition Insurance Solutions Pty Ltd. | Australia | 657140791 | Level 16<br>80 Collins Street, South Tower<br>Melbourne VIC, 3000 Australia | privacy@coalitioninc.com |
| Coalition Insurance Solutions GmbH | Germany | HRB 133708 | Thurn-und Taxis-Platz 6<br>D-60313 Frankfurt, Germany | privacy@coalitioninc.com |
| Coalition Incident Response UK, Ltd. | United Kingdom | 14121267 | 34-36 Lime<br>Street London EC3M 7AT,<br>United Kingdom | privacy@coalitioninc.com |

| | | | | |
|---|---|---|---|---|
| Coalition Incident Response Canada, Inc. | Canada | 705272474BC0001 | 1600 Cathedral Place - 925 West Georgia Street, Vancouver, BC V6C 3L2, Canada | privacy@coalitioninc.com |
| Coalition Insurance Solutions Canada, Inc. | Canada | 797705076BC0001 | 1600 Cathedral Place - 925 West Georgia Street, Vancouver, BC V6C 3L2, Canada | privacy@coalitioninc.com |
| Coalition Insurance Company | United States of America | 133368745 (NY) | 19 West 44th Street, 15th Floor, New York, New York 10036 | privacy@coalitioninc.com |
| Affinity Partners Insurance Solutions, LLC | United States of America | 931573355 (DE) | 250 W Center Street Suite 320, Provo, UT 84601 | privacy@coalitioninc.com |
| Coalition Reinsurance Services, LLC | United States of America | 933164659 (DE) | 55 2nd Street, Suite 2500, San Francisco, CA 94105 | privacy@coalitioninc.com |
| Palekana Solutions Holdings, Inc. | United States of America | 854136208 (HI) | 201 Merchant St., Suite 2400 Honolulu, Hawai'i 96813 | privacy@coalitioninc.com |
| Palekana Insurance, Inc. | United States of America | 854166477 (HI) | 201 Merchant St., Suite 2400 Honolulu, Hawai'i 96813 | privacy@coalitioninc.com |

## Exhibit 4 – Controller Sub-Processors

The Controller has authorised the use of the following sub-processors:

| Subprocessor | Use Case | Processing Location |
|---|---|---|
| AgentSync, Inc. | Management of broker and agent information. | United States |
| Amazon Web Services, Inc. | Hosting and storage systems provider. | United States |
| Argus West, Inc. | Compliance training platform. | United States |
| Catamorphic, Co. d/b/a LaunchDarkly | Development feature flagging and platform management. | United States |
| Centiment LLC | Conducts surveys for targeted audiences, including Coalition clients. | United States |
| Chameleon.io | Platform that enables the building of product experiences, walk-throughs, tooltips and announcements to improve UX. | United States |
| Channelscaler | Client engagement and ecosystem growth platform. | United States |
| Chargebee Technologies Private Limited | Billing platform for Coalition Control products. | India |
| Chili Piper, Inc. | Scheduling application for engagement with brokers. | United States |
| Clickhouse, Inc. | Hosting and storage systems provider | United States |
| Contentful GmbH | Web hosting for various sites. | Germany |
| ECE Consulting Group, Inc. a/k/a ECE Contact Centers, Inc. | Customer service, technical support and data entry. | Philippines |
| eWebinar Labs | Webinar platform for hosting external broker platforms. | United States |
| Experian Information Solutions, Inc. | Data factor (credit score) for issuing quotes. | United States |
| Github Inc. | Cloud-based service for software development. | United States |

| Subprocessor | Use Case | Processing Location |
|---|---|---|
| Gong.io Ltd | Intelligence platform capturing conversations for the purpose of analysis. | United States |
| Google LLC | G Suite, Google Analytics, LLM hosting and Looker. | United States |
| Hubspot, Inc. | CRM, client management. | United States |
| IDB, LLC | IP address enrichment | United States |
| Intercom | Support and user guides | Dependent on client configuration |
| Ironclad, Inc. | Contract management and storage. | United States |
| Lob.com, Inc. | Direct mail SaaS platform. | United States |
| Loom, Inc. | Platform for creating training content and videos. | United States |
| Marketo, Inc. | Marketing automation software. | United States |
| Mentimeter AB | Real-time polls for slide decks. | Sweden |
| Microsoft Azure | Hosting and storage systems provider | Dependent on client location |
| Netsuite Inc. | Accounting and leads software. | United States |
| Okta, Inc. | Authentication/SSO application. | United States |
| OneTrust, LLC | Website cookie banner. | United States |
| OpenAI | AI application. | United States |
| Outreach Corporation | Sales engagement. | United States |
| Pandadoc Inc. | Document signing application. | United States |
| Rocket Science Group, LLC d/b/a Mailchimp | Email platform used to communicate with brokers and policyholders. | United States |
| Salesforce, Inc. | CRM | United States |
| SentinelOne, Inc. | Endpoint detection response tool for investigations and managing clients. | United States |
| ShareFile, LLC | Secure file sharing. | United States |
| Slack Technologies, Inc. | Internal messaging; external | United States |

| Subprocessor | Use Case | Processing Location |
|---|---|---|
| | with consent. | |
| Snowflake Inc. | Cloud-based database. | United States |
| Stripe, Inc. | Payment collection used for subscription plans. | United States |
| Superlative Enterprises Pty Ltd | Threat and exposure intelligence | Australia |
| Sutro Labs, Inc. | Reverse ETL tool, moves data from warehouse to Salesforce CRM. | United States, Germany |
| Twilio, Inc. | Sales outreach. | United States |
| Vertafore, Inc. | Agency management software. | United States |
| WeWork | Flexible office and coworking spaces. | United States, Canada, Germany, UK, Australia |
| Wizer Inc. | Information Security training partner. | United States |
| Zendesk, Inc. | Platform and services for support ticket management. | United States |

In addition to the subprocessors listed above, the following entities are part of the Coalition group, and accordingly may also function as subprocessors in order to provide Coalition's products and services:

| Entity Name | Processing Location |
|---|---|
| BinaryEdge, AG | Switzerland |
| Coalition - Deiniram Doluções de Segurança, Unipessoal, Lda. | Portugal |
| Coalition Incident Response, Inc. | United States |
| Coalition Insurance Solutions GmbH | Germany |
| Coalition Insurance Solutions, Inc. | United States |
| Coalition Insurance Solutions Pty Ltd. | Australia |
| Coalition Risk Solutions Ltd. | United Kingdom |


Coalition®