

DATA PROCESSING ADDENDUM

Last updated November 21, 2025

This Data Processing Addendum, including all schedules and attachments hereto (“DPA”) is governed by and part of that certain written agreement executed between Subscriber and RampedUp, LLC (“RampedUp”), such as the parties’ Service Subscription Agreement, Terms of Service, or any other written agreement between the parties for provision of the RampedUp Services to Subscriber (in each case, the “Agreement”). RampedUp and Subscriber may each be referred to herein as a “Party” or collectively as the “Parties.” Capitalized terms not defined herein have the same meaning set forth in the Agreement.

This DPA consists of:

- **Section I:** Defined Terms applicable to all Processing of Personal Data under the Agreement.
- **Section II:** Processing RampedUp Data, which applies only if and to the extent that Subscriber uses RampedUp Services.
- **Section III:** Processing Subscriber Personal Data, which applies only if and to the extent that Subscriber uses RampedUp Services via API or the user platform.
- **Section IV:** General Terms and Conditions applicable to all Processing of Personal Data under the Agreement.
- **Schedules 1 and 2,** governing cross-border transfers of European Personal Data, as applicable.

BY EXECUTING THE AGREEMENT, THE PARTIES AGREE TO THE TERMS AND CONDITIONS IN THIS DPA IN CONNECTION WITH THE PROCESSING OF PERSONAL DATA THAT OCCURS AS PART OF RAMPEDUP’S PROVISION OF THE RAMPEDUP SERVICES TO SUBSCRIBER.

Additionally, and for the avoidance of doubt, Subscriber’s execution of the Agreement shall be deemed to constitute Subscriber’s signature and acceptance of the applicable Standard Contractual Clauses and all other schedules and exhibits attached hereto. RampedUp’s Data Protection Officer may be reached at privacy@rampedup.io.

SECTION I: DEFINED TERMS

For purposes of this DPA, the following terms have the meanings given below:

1. Definitions

- a. **“Affiliate”** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control” for purposes of this definition means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.

b. **“Applicable Laws”** means all laws, rules, regulations, and orders applicable to the subject matter herein, including without limitation Data Protection Laws.

c. **“Business”, “Sell”, “Share”, and “Service Provider”** shall have the meanings given to them in the CCPA and other Data Protection Laws, as applicable.

d. **“Consumer”** means the natural person to whom the Personal Data relates.

e. **“Controller”** means the entity which determines the means and purposes of the Processing of Personal Data.

f. **“Data Protection Laws”** means all applicable federal, state, and local legislation relating to data protection and privacy that apply to the Processing of Personal Data under the Agreement, including without limitation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), together with any subordinate legislation or implementing regulation and other laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom (collectively, **“European Data Protection Laws”**), and U.S. federal and state laws governing consumer privacy and data protection such as California Civil Code Sec. 1798.100 et seq., also known as the California Consumer Privacy Act of 2018, as amended (**“CCPA”**); in each case as amended, superseded, or replaced from time to time.

g. **“Data Subject”** means the identified or identifiable person to whom Personal Data relates, including as applicable any “Consumer” as that term is defined by the CCPA and certain other United States Data Protection Laws.

h. **“Europe”** means the European Union, the European Economic Area, Switzerland, and the United Kingdom.

i. **“Personal Data”** means information describing or relating to an identified or identifiable natural person or household or an identified or identifiable legal entity and where such information is protected as personal data or personally identifiable information under applicable Data Protection Laws.

j. **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. A Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, such as failed log-in attempts, pings, port scans, denial-of-service attacks, or other network attacks on firewalls or networked systems. A Personal Data Breach also does not include the disclosure of information that is already publicly available.

k. **“Process” or “Processing”** means any operation or set of operations which is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

l. **“Processor”** means the party that Processes Personal Data on behalf of the Controller, including as applicable any “Service Provider” as that term is defined by the CCPA and similar Data Protection Laws.

m. **“Standard Contractual Clauses”** or **“SCCs”** means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

n. **“Sub-Processor”** means a Processor engaged by RampedUp to perform services under the Agreement on behalf of RampedUp.

SECTION II: PROCESSING RAMPEDUP DATA

This Section II applies to Subscriber’s use of RampedUp Services that result in Subscriber receiving or Processing Personal Data contained within **RampedUp Data**.

1. **Roles of Parties.** Each Party shall act as a separate and independent Controller (and not as a joint Controller) in relation to any Personal Data contained in the RampedUp Data that Subscriber receives from RampedUp or further Processes pursuant to the Agreement or that Subscriber transfers from RampedUp’s systems or APIs.
2. **Compliance with Law.** Each Party shall comply with all Data Protection Laws in respect of its Processing of Data and shall ensure that it has a lawful basis for all such Processing, where applicable. Where an Affiliate of a Party is a Controller or Processor of Data under this Agreement, such Party shall ensure that its Affiliate complies with its obligations under the Data Protection Laws and this DPA as applicable.
3. **Assistance; Notifications.** Each Party will provide the other Party with (a) reasonable cooperation, assistance, and information to assist that other Party with its compliance with Data Protection Laws, and (b) reasonable assistance in complying with any Consumer or Data Subject request to exercise their rights under applicable Data Protection Laws (**“Privacy Request”**). Each Party shall promptly notify the other (to the extent permitted by law) in writing, providing reasonable details of any third-party complaint, audit, investigation, or enquiry establishing, alleging, or enquiring as to possible non-compliance with any Applicable Laws in connection with Personal Data maintained by or for such Party, and the Parties will cooperate reasonably with each other in respect thereof.
4. **Processing By Subscriber.** Subscribers receive or Process Data as a Controller (and/or Business, as applicable) pursuant to Subscriber’s own privacy practices. Subscriber shall provide the same level of privacy protection to Data as required by Data Protection Laws. Subscriber is solely responsible for: (a) providing all Consumers and Data Subjects with legally adequate notice and consent of Subscriber’s Processing of Data; (b) the security of Data that Subscriber receives from RampedUp; and (c) compliance with Privacy Requests regarding Data on Subscriber’s information systems. The Parties acknowledge and agree that Subscriber’s receipt of Data may qualify as a Sale or Sharing of Personal Data under applicable Data Protection Laws and any and all further Processing of Data

by Subscriber is Subscriber's sole responsibility and subject to Subscriber's privacy practices.

RampedUp has the right to take reasonable and appropriate steps to help ensure that Subscriber uses Data in a manner consistent with Subscriber's obligations under relevant Data Protection Laws. Subscriber shall notify RampedUp if Subscriber determines that it can no longer meet its obligations under relevant Data Protection Laws, and upon such notification, RampedUp has the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Data. Subscriber will direct Data Subjects to the RampedUp **DO NOT SELL / Opt-Out** portal: <https://basic.rampedup.io/app/donotsell>.

5. **Transfers of European Personal Data.** Module One: Transfer controller to controller of the Standard Contractual Clauses attached hereto as **Schedule 1** applies only if and to the extent that Subscriber's use of the RampedUp Services under this Section II includes the transfer of European Personal Data out of Europe to a country which does not ensure an adequate level of data protection within the meaning of the European Data Protection Laws. Schedule 1 can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws of Europe.
6. **Personal Data Breach.** Subscriber shall immediately notify RampedUp of: (i) any breach of security or unauthorized access to Data that Subscriber detects or becomes aware of; (ii) any Data Subject requests to access, delete, release, correct, or block access to Data; or (iii) any other complaint, inquiry, or request from a Consumer or government or regulatory agency regarding Data, unless such notice is prohibited by law.

SECTION III: PROCESSING SUBSCRIBER PERSONAL DATA

This Section III applies to any and all Processing of Personal Data contained in **Subscriber Data** or **Subscriber Materials** (in either case, as defined in the Agreement) ("**Subscriber Personal Data**") by RampedUp on behalf of Subscriber pursuant to the Agreement.

1. **Roles of Parties.** The Parties acknowledge and agree that (a) with regard to the Processing of Subscriber Personal Data, Subscriber is the Controller and RampedUp is the Processor, in each case as those terms are defined in applicable Data Protection Laws.
2. **Duration.** RampedUp shall Process Subscriber Personal Data throughout the duration of the term of the Agreement or any renewal term thereof. Upon termination of RampedUp Services by either Party, RampedUp shall cease Processing Subscriber Personal Data on Subscriber's behalf upon completion of the termination provisions described herein.
3. **Nature, Purpose, and Subject-Matter of the Processing.** The nature and purpose of RampedUp's Processing of Subscriber Personal Data is described in and governed by the Agreement. The subject matter of data Processed under this DPA is Subscriber Personal Data of Subscriber's customers, potential customers, employees, contractors, representatives, and other Data Subjects as otherwise described in the Agreement. The nature and purpose of the Processing, the categories of Personal Data, and Consumers/Data Subjects Processed under this DPA are further specified in **Schedule 2** hereto.

4. **Processing By RampedUp.** Subscriber hereby appoints RampedUp to Process the Personal Data contained in Subscriber Data on behalf of Subscriber as necessary for RampedUp to provide the RampedUp Services under the Agreement. All Personal Data Processed under the Agreement (including this DPA) will be stored, organized, and made available to Subscriber as the Controller. RampedUp shall treat Personal Data as Confidential Information. If RampedUp is required by applicable law to disclose Subscriber Data for a purpose unrelated to the Agreement, RampedUp will first inform Subscriber of the legal requirement and give Subscriber an opportunity to object or challenge the requirement, unless the law prohibits such notice.

Notwithstanding the foregoing, RampedUp shall have the right to collect and use Personal Data contained in Subscriber Data to investigate a use of the Service that is unlawful or violates the Agreement, to provide and develop the Service, to respond to legal actions, or for administrative purposes such as accounting and compliance.

5. **Instructions.** RampedUp shall Process, retain, use, store, or disclose Subscriber Personal Data only according to written, documented instructions issued by Subscriber to RampedUp to perform a specific or general action with regard to Personal Data for the purpose of providing the RampedUp Services to Subscriber pursuant to the Agreement (“**Instructions**”). The Parties agree that the Agreement, together with Subscriber’s use of the RampedUp Services in accordance with the Agreement, constitute Subscriber’s complete and final Instructions to RampedUp in relation to the Processing of Subscriber Personal Data.

Subscriber may modify, amend, add, or replace individual Instructions in writing (“**Additional Instructions**”) by email to Subscriber’s designated RampedUp contact. Any Additional Instructions must be consistent with this DPA and the Agreement. If RampedUp determines that Additional Instructions are outside the scope of the Agreement, RampedUp may charge additional fees and/or require a written agreement between RampedUp and Subscriber to perform such Additional Instructions. RampedUp shall inform Subscriber without delay if, in RampedUp’s opinion, an Instruction violates applicable Data Protection Laws or RampedUp is unable to follow an Instruction and, where necessary, cease all Processing until Subscriber issues new Instructions with which RampedUp is able to comply.

6. **Limitations of Processing.** The Parties agree that RampedUp will Process Subscriber Personal Data as a Service Provider or Processor strictly for the business purpose of providing the RampedUp Services under the Agreement and as set forth in RampedUp’s Privacy Policy (<https://rampedup.io/privacy-policy-1>). The Parties agree that RampedUp shall not:
 - a. Sell or Share (as those terms are defined in the CCPA) the Subscriber Personal Data;
 - b. retain, use, or disclose Subscriber Personal Data for RampedUp’s own commercial purpose except as permitted by the Agreement and applicable Data Protection Laws; or
 - c. retain, use, or disclose Subscriber Personal Data outside of the direct business relationship between Subscriber and RampedUp.

RampedUp hereby certifies that it understands and will comply with the restrictions of this Section III(6).

7. **Subscriber Obligations.** Subscriber shall, in its use of RampedUp Services, Process Subscriber Personal Data in accordance with the requirements of all applicable Data Protection Laws, including without limitation requirements to provide notice to Data Subjects of the use of RampedUp as Processor. Subscriber shall have sole responsibility for:
- a. the accuracy, quality, and legality of Subscriber Personal Data and the means by which Subscriber acquires such data;
 - b. complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of Personal Data, including obtaining any necessary consents and authorizations;
 - c. ensuring Subscriber has the right to transfer or provide access to the Subscriber Personal Data to RampedUp for Processing in accordance with the Agreement (including this DPA);
 - d. ensuring that Subscriber's Instructions to RampedUp regarding the Processing of Subscriber Personal Data comply with Data Protection Laws; and
 - e. using the Services in compliance with Data Protection Laws.

Subscriber represents and warrants that Subscriber has established a lawful basis to Process Personal Data, Subscriber's use of the RampedUp Services will not violate the rights of any Data Subject, and Subscriber has the right to transfer, or provide access to, the Personal Data to RampedUp for Processing in accordance with the terms of the Agreement. Subscriber shall inform RampedUp without undue delay if Subscriber is unable to comply with its obligations under this DPA or Data Protection Laws. For the avoidance of doubt, RampedUp is not responsible for compliance with any Data Protection Laws applicable to Subscriber or Subscriber's industry that are not generally applicable to RampedUp.

8. **Subscriber Does Not Sell or Share Subscriber Personal Data to RampedUp.** The Parties agree that Subscriber does not Sell or Share the Subscriber Personal Data that RampedUp Processes on behalf of Subscriber to RampedUp because, as a Service Provider or Processor, RampedUp may only use Subscriber Personal Data for the purposes of providing the Services to Subscriber.
9. **RampedUp Personnel.** RampedUp shall (a) ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data; (b) take commercially reasonable steps to ensure the reliability of any RampedUp personnel engaged in the Processing of Personal Data; and (c) limit RampedUp personnel access to Subscriber Personal Data to those personnel who are necessary to provide the RampedUp Services.
10. **Sub-Processors.** Subscriber authorizes RampedUp to engage the Sub-Processors on RampedUp's Sub-Processor List (defined below) as of the Effective Date to Process Subscriber Data pursuant to the Agreement (including this DPA) and Subscriber acknowledges and agrees that: (a) RampedUp's Affiliates may be retained as Sub-Processors; and (b) RampedUp may engage third-party Sub-Processors in connection with the provision of the RampedUp Services.

RampedUp or a RampedUp Affiliate has entered into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Subscriber Data to the extent applicable to the nature of the RampedUp Services provided by such Sub-Processor. RampedUp shall be liable for the acts and omissions of its Sub-Processors to the same extent RampedUp would be liable if performing the

RampedUp Services of each Sub-Processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

RampedUp shall maintain and keep up to date a current list at <https://rampedup.io/sub-processors> (the “Sub-Processor List”). RampedUp shall give Subscriber at least thirty (30) days’ prior written notice (such notice shall be via an email alert, which Subscriber may subscribe to on the Sub-Processor List webpage) if RampedUp engages a new Sub-Processor that will process Personal Data pursuant to the Agreement. Subscriber may object to RampedUp’s use of a new Sub-Processor by notifying RampedUp promptly in writing within ten (10) business days after receipt of such notice.

In the event Subscriber objects to a new Sub-Processor, as permitted in the preceding sentence, RampedUp will use reasonable efforts to make available to Subscriber a change in the RampedUp Services or recommend a commercially reasonable change to Subscriber’s configuration or use of the RampedUp Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening Subscriber. If RampedUp is unable to make available such change within thirty (30) days of the objection notice, Subscriber may terminate the Agreement with respect only to those Services which cannot be provided by RampedUp without the use of the objected-to new Sub-Processor by providing written notice to RampedUp.

11. **Privacy Requests.** RampedUp shall, to the extent legally permitted, promptly notify Subscriber if RampedUp receives a Privacy Request related to Subscriber Personal Data. If Subscriber is unable to independently address the Privacy Request, RampedUp will assist Subscriber by appropriate technical and organizational measures, insofar as this is possible and to the extent RampedUp is legally permitted to do so, for the fulfilment of Subscriber’s obligation to respond to a Data Subject Request under Data Protection Laws. Subscriber shall be legally responsible for responding substantively to all such Privacy Requests or communications involving Subscriber Personal Data and for all costs associated with the same.
12. **Transfers of European Subscriber Personal Data.** Module Two: Transfer controller to processor of the Standard Contractual Clauses attached hereto as **Schedule 2** applies only if and to the extent that Subscriber’s use of the RampedUp Services under this Section III includes the transfer of European Personal Data out of Europe to a country which does not ensure an adequate level of data protection within the meaning of the European Data Protection Laws. Schedule 2 can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws of Europe.
13. **Impact of Local Laws.** As of the Effective Date, RampedUp has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Subscriber Personal Data as described in the Agreement, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent RampedUp from fulfilling its obligations under this DPA. If RampedUp reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of Subscriber Personal Data (“Local Laws”) prevent it from fulfilling its obligations under this DPA, it shall promptly notify Subscriber.

In such a case, RampedUp shall use reasonable efforts to make available to Subscriber a change in the RampedUp Services or recommend a commercially reasonable change to Subscriber’s configuration or use of the RampedUp Services to facilitate compliance with the Local Laws without unreasonably burdening Subscriber. If RampedUp is unable to make available such

change promptly, Subscriber may terminate the Agreement and suspend the transfer of Subscriber Personal Data in respect only to those Services which cannot be provided by RampedUp in accordance with the Local Laws by providing written notice in accordance with the notice requirements of the Agreement.

14. **Government Access Requests.** If RampedUp receives a legally binding request from a government agency, state body, court, or other public authority (“Public Authority”) to access Subscriber Personal Data (“**Government Access Request**”), RampedUp shall, unless otherwise legally prohibited, promptly notify Subscriber including a summary of the nature of the request.

To the extent RampedUp is prohibited by law from providing such notification, RampedUp shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable RampedUp to communicate as much information as possible, as soon as possible. Further, RampedUp shall challenge the request if it concludes that there are reasonable grounds to consider that the request is unlawful. When challenging a request, RampedUp shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits.

RampedUp shall not disclose the Subscriber Personal Data requested until required to do so under the applicable procedural rules. RampedUp agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. RampedUp shall promptly notify Subscriber if RampedUp becomes aware of any direct access by a Public Authority to Subscriber Personal Data and provide information available to RampedUp in this respect, to the extent permitted by law.

For the avoidance of doubt, this DPA shall not require RampedUp to pursue action or inaction that could result in civil or criminal penalty for RampedUp such as contempt of court.

15. **Impact Assessment; Demonstration of Compliance.** To the extent RampedUp is required under Data Protection Laws, RampedUp shall (at Subscriber's expense) provide reasonably requested information regarding RampedUp's Processing of Subscriber Personal Data to enable Subscriber to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

Upon Subscriber's written request and with at least thirty (30) days' notice (or a shorter period if permitted by Applicable Law), RampedUp shall make available to Subscriber on a confidential basis all reasonably necessary information and allow for and contribute to audits to demonstrate RampedUp's compliance with this DPA, provided that Subscriber shall not exercise this right more than once per year. Such audits shall be solely in the form of information relating to the Processing under this DPA as provided by documents and interviews with RampedUp information technology employees and subcontractors or applicable third parties. No access to any part of RampedUp's information system, data hosting sites or centers, or infrastructure will be permitted.

Subscriber or its designated and professionally qualified agent may carry out such audit. Subscriber must conduct all audits (a) during normal business hours; (b) according to RampedUp's security and confidentiality terms and guidelines; and (c) taking reasonable measures necessary to prevent unnecessary disruption to RampedUp's operations. Subscriber shall be responsible for all costs and expenses arising from audits, including the actual costs and

expenses of RampedUp in complying with an audit request. Subscriber shall take all reasonable measures to limit any impact on RampedUp by combining several information or audit requests in one single request.

16. **Personal Data Breach.** RampedUp will notify Subscriber without undue delay after RampedUp becomes aware of a known or suspected likely Personal Data Breach involving Subscriber Personal Data and will provide timely information relating to such Personal Data Breach as it becomes known or as reasonably requested by Subscriber. At Subscriber's request, RampedUp will promptly provide Subscriber with commercially reasonable assistance as necessary to enable Subscriber to notify authorities and/or affected Consumers, if Subscriber is required to do so under Data Protection Laws. The obligations of this Section III(16) do not apply to incidents that are caused by Subscriber or its end users.
17. **Deletion or Return of Subscriber Personal Data.** At the expiry or termination of the Agreement, RampedUp will, at Subscriber's option, delete or return to Subscriber all Subscriber Personal Data Processed pursuant to this DPA in accordance with Subscriber's reasonable Instructions. The requirements of this Section III(17) shall not apply to the extent that RampedUp is required by Applicable Law to retain some or all of the Subscriber Personal Data, or to Subscriber Personal Data RampedUp has archived on back-up systems, which data RampedUp shall securely isolate and protect from any further Processing and delete in accordance with RampedUp's deletion practices.

SECTION IV: GENERAL TERMS & CONDITIONS

This Section IV applies to any and all Processing by the Parties pursuant to the Agreement.

1. **Restriction on Sensitive Personal Data.** The Parties acknowledge and agree that neither Party shall provide or make available sensitive Personal Data to the other Party in connection with the Services. The Parties acknowledge and agree that RampedUp shall have no responsibility or liability for any sensitive Personal Data erroneously or inadvertently transferred under this DPA.
2. **Data Ownership.** Nothing in this DPA shall be construed to convey any ownership interest or license in the Personal Data that is contrary to the ownership interests and licenses set forth in the Agreement.
3. **Security.** Each Party shall implement appropriate technical and organizational security measures (including maintaining any security controls) designed to ensure a level of security for Personal Data in such Party's possession or control that is appropriate to the risk presented by the Processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to such Personal Data transmitted, stored or otherwise Processed. Subscriber is solely responsible for (i) determining whether the RampedUp Services meet Subscriber's security standards and support Subscriber's obligations under Data Protection Laws and (ii) the secure use of RampedUp's Services by Subscriber or any individual Subscriber

provides with a device listed on or access to Subscriber's account, including but not limited to securing account authentication information and ensuring no end user of Subscriber seeks to misuse Personal Data or engages in activities likely to give rise to a Personal Data Breach.

4. **Authorized Affiliates.** The Parties acknowledge and agree that, by executing the Agreement, Subscriber executes this DPA on behalf of itself and, as applicable, on behalf of its Affiliates that Subscriber has permitted to use the RampedUp Services pursuant to the Agreement ("**Authorized Affiliates**"), thereby establishing a separate DPA between RampedUp and each such Authorized Affiliate subject to the provisions of the Agreement and this Section IV(4).

Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a Party to the Agreement and is only a Party to the DPA. All access to and use of the RampedUp Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Subscriber.

As the contracting Party to the Agreement, Subscriber shall remain responsible for coordinating all communication with RampedUp under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates. Where an Authorized Affiliate becomes a Party to the DPA with RampedUp, except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against RampedUp directly by itself, solely Subscriber as the contracting Party to the Agreement shall exercise any right or seek any such remedy on behalf of the Authorized Affiliate and shall exercise any such rights under this DPA in a combined manner for itself and all of its Authorized Affiliates together, not separately for each Authorized Affiliate individually.

5. **Limited Liability.** Except as specifically provided in the Standard Contractual Clauses hereto, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and RampedUp, whether in contract, tort, or under any other theory of liability, is subject to the limitations of liability set forth in the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, RampedUp's and its Affiliates' total liability for all claims from Subscriber and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Subscriber and all of its Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Subscriber and/or any Authorized Affiliate that is a contractual Party to any such DPA.

6. **Miscellaneous.** In case of any conflict or inconsistency with the terms of the Agreement, this DPA shall take precedence over the terms of the Agreement to the extent of such conflict or inconsistency. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

RampedUp may periodically update this DPA; Subscriber will be informed of any modification by email, alert on the Services, or other means and Subscriber's continued use of the RampedUp Services following such update shall be Subscriber's agreement thereto.

Schedule 1

Controller-to-Controller Transfer Mechanisms for European Data Transfers

This Schedule 1 applies only if and to the extent that Subscriber's use of the RampedUp Services under Section II of the DPA includes the transfer of European Personal Data out of Europe to a country which does not ensure an adequate level of data protection within the meaning of the European Data Protection Laws.

1. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

For the purposes of Section II of the DPA and Module One controller to controller transfer clauses ("C-to-C Transfer Clauses"), RampedUp is the data exporter, and Subscriber is the data importer, and the Parties agree to the following. If and to the extent an Authorized Affiliate relies on the C-to-C Transfer Clauses for the transfer of Personal Data, any references to "Subscriber" in this Schedule, include such Authorized Affiliate. Where this Schedule 1 does not explicitly mention C-to-C Transfer Clauses it applies to them. The relevant provisions contained in Module One of the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Annex 1 to this Schedule 2. Where transfer of Personal Data between the parties under Section II of this DPA is a Restricted Transfer and European Data Protection Laws require that appropriate safeguards are put in place, such transfers shall be subject to the Standard Contractual Clauses, which shall be deemed incorporated into and form part of the DPA, as follows:

1) EU C-to-C Transfers

- a) Module One (Controller to Controller) will apply.
- b) Clause 7, the optional docking clause will not apply.
- c) Clause 11, the optional language will not apply.
- d) Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law.
- e) Clause 18(b), disputes shall be resolved before the courts of Ireland.
- f) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this Schedule 1 (as applicable to the Restricted Transfer in question); and
- g) Annex II of this Schedule 1 shall be deemed completed with the information set out in Annex 2 to this DPA.

2) UK Transfers: In relation to transfers of Personal Data that are protected by UK Privacy Laws, the EU SCCs:

- a) shall apply as completed in accordance with paragraphs (a) and (b) above; and

b) shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the parties and incorporated into and form an integral part of this DPA.

Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex 1 and 2 of this Schedule 1 and table 4 in Part 1 shall be deemed completed by selecting "neither party".

3) Swiss Transfers: In relation to transfers of Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraph (a) and (b) above, with the following modifications:

a) references "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

b) references to specific Articles "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

c) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law";

d) the term "member state" shall 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 (i.e., Switzerland);

e) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

f) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

g) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

h) Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

4) Alternative Transfers: To the extent RampedUp adopts an alternative recognized lawful mechanism for the transfer of Personal Data not described in this DPA ("Alternative Transfer Mechanism"), RampedUp will provide written notice to Subscriber and upon such notice the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Personal Data is transferred).

Annex 1 to Schedule 1

Description of the Processing Activities / Transfer

I. ANNEX 1(B) PARTIES

a. Data Exporter: RampedUp, Inc. with respect to Processing of Personal Data described in Section II of the DPA.

Address: P.O. Box 88129 Atlanta, GA 30356

Contact: scott.miller@rampedup.io

b. Data Importer: Subscriber, as identified in the Agreement, with respect to Processing of Personal Data described in Section II of the DPA.

Address: As specified in the Agreement or Subscriber's account

Contact: the contact details associated with Subscriber's account, or as otherwise specified in the Agreement.

c. Activities relevant to the transfer: See Annex 1(B) below Activities relevant to the transfer: See Annex 1(B) below.

d. Signature and date: The parties' execution of the Agreement shall constitute execution of the Standard Contractual Clauses by both parties.

II. ANNEX 1(B) DESCRIPTION OF TRANSFER

a. Controller Data: Module 1 (Controller to Controller)

b. Categories of data subjects: Subscriber's employees, consultants, contractors, or agents or professional business-to-business contacts or other natural persons related to Subscriber's business activities as determined by Subscriber.

c. Purposes of the transfer(s): The transfer is made to provide Subscriber with the RampedUp Services, including but not limited to access to RampedUp's databases for Subscriber's business-to-business activities. For further information, please review the RampedUp Privacy Policy <https://rampedup.io/privacy-policy-1>

d. Categories of personal data: Publicly available professional contact information about the Data Subject, including:

- Identifiers
- Employment-related information
- Commercial information
- Internet or similar activity

e. Sensitive Data: None. The personal data transferred concerns the following categories of sensitive data: N/A

f. Frequency of the transfer: Continuous

g. Nature of the Processing: As described in the Agreement.

h. Retention period (or, if not possible to determine, the criteria used to determine that period): RampedUp will not retain Personal Data for longer than the period during which RampedUp has

a legitimate need to retain Personal Data for purposes it was collected or transferred. See Privacy Policy for details.

Schedule 2

Controller-to-Processor Transfer Mechanisms for European Data Transfers

This Schedule 2 applies only if and to the extent that Subscriber's use of the RampedUp Services under Section I II of the DPA includes the transfer of European Personal Data out of Europe to a country which does not ensure an adequate level of data protection within the meaning of the European Data Protection Laws.

2. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

For the purposes of the Section III of the DPA and Module Two controller to processor transfer clauses ("C-to-P Transfer Clauses"), Subscriber is the data exporter and RampedUp is the data importer, and the Parties agree to the following. If and to the extent an Authorized Affiliate relies on the C-to-P Transfer Clauses for the transfer of Personal Data, any references to "Subscriber" in this Schedule, include such Authorized Affiliate. Where Schedule 2 does not explicitly mention C-to-P Transfer Clauses it applies to them.

2.1. Reference to the Standard Contractual Clauses. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Appendix 1 to this Schedule 2.

2.2. Docking clause. The option under clause 7 shall not apply.

2.3. Certification of Deletion. The Parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by RampedUp to Subscriber only upon Subscriber's written request.

2.4. Instructions. This DPA and the Agreement are Subscriber's complete and final documented instructions at the time of signature of the Agreement to RampedUp for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Subscriber to Process Personal Data are set out in Section III (5) of this DPA and include onward transfers to a third Party located outside Europe for the purpose of the provision of the RampedUp Services.

2.5. Security of Processing. For the purposes of clause 8.6(a), Subscriber is solely responsible for making an independent determination as to whether the technical and organizational measures set forth in the RampedUp Privacy Policy and applicable RampedUp policies governing data security and protection and Subscriber agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by RampedUp provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with Section III (16) of this DPA.

2.6. Audits of the SCCs. The Parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section III (15) of this DPA.

2.7. General authorization for use of Sub-processors. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), RampedUp has Subscriber's general authorization to engage Sub-processors in accordance with Section III (10) of this DPA. RampedUp shall make available to Subscriber the current list of Sub-processors in accordance with Section III (10) of this DPA. Where RampedUp enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the RampedUp Services, Subscriber grant RampedUp authority to provide a general authorization on Controller's behalf for the engagement of Sub-processors by Sub-processors engaged in the provision of the RampedUp Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.
<https://rampedup.io/sub-processors>

2.8. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to clause 9(a), Subscriber acknowledges and expressly agrees that RampedUp may engage new Sub-processors as described in Sections III (10) of this DPA. RampedUp shall inform Subscriber of any changes to Sub-processors following the procedure provided for in Section III (10) of this DPA. 2.9. Complaints-Redress. For the purposes of clause 11, and subject to Section III (11) of this DPA, RampedUp shall inform data subjects on its website of a contact point authorized to handle complaints. RampedUp shall inform Subscriber if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Subscriber. RampedUp shall not otherwise have any obligation to handle the request (unless otherwise agreed with Subscriber). The option under clause 11 shall not apply.

2.10. Liability. RampedUp's liability under clause 12(b) shall be limited to actual and proven damage caused by RampedUp's Processing of Personal Data on Subscriber's behalf as a Processor where RampedUp has not complied with its obligations under the GDPR specifically directed to Processors, or where RampedUp has acted outside of or contrary to Subscriber's lawful Instructions, as specified in Article 82 GDPR.

2.11. Supervision. Clause 13 shall apply as follows:

2.11.1. Where Subscriber is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Subscriber with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

2.11.2. Where Subscriber is not established in an EU Member State, but fall within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and have appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

2.11.3. Where Subscriber is not established in an EU Member State, but fall within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative 11 pursuant to Article 27(2) of Regulation (EU) 2016/679 : The Data Protection Commission of Ireland, 21 Fitzwilliam Square South, Dublin, 2 D02 RD28, Ireland shall act as competent supervisory authority.

2.11.4. Where Subscriber is established in the United Kingdom or fall within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as competent supervisory authority.

2.11.5. Where Subscriber is established in Switzerland or fall within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws.

2.12. Notification of Government Access Requests. For the purposes of clause 15.1(a), RampedUp shall notify Subscriber only, and not the Data Subject(s), in case of government access requests. Subscribers shall be solely responsible for promptly notifying the Data Subject as necessary.

2.13. Governing Law. The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

2.14. Choice of forum and jurisdiction. The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the Parties agree that the courts of either (i) Ireland ; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

2.15. Appendix. The Appendix shall be completed as follows:

- The contents of section 1 of Appendix 1 to Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Appendix 1 to Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Appendix 1 to Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Appendix 1 to Schedule 2 to this Exhibit shall form Annex II to the S CCs.

2.16. Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses. In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws of Switzerland (“Swiss Data Protection Laws”), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws of the United Kingdom (“UK Data Protection Laws”) or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses 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.

2.17. Conflict. The Standard Contractual Clauses are subject to this DPA, and the additional safeguards are set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

Appendix 1 to Schedule 2

Description of Processing/Transfer

1. LIST OF PARTIES

Data exporter(s): Subscriber as identified in registration.

Address: Subscriber's address listed in registration

Role: For the purposes of the SCCs, Subscriber is a Controller.

Activities relevant to the data transferred under these clauses: Provision of the RampedUp Services pursuant to the Agreement (including the DPA). Contact person's name, position, and contact details: Subscriber's designated point of contact listed at registration Signature: By agreeing to the Agreement and the DPA, Subscriber agrees to this Appendix 1 to Schedule 2, effective as of the date of the Agreement.

Role: For the purposes of the C-to-P Transfer Clauses Subscriber and/or Subscriber's Authorized Affiliates are a Controller.

Data Importer(s): RampedUp, Inc.

Address: P.O. Box 88129 Atlanta, GA 30356

Contact person's name, position, and contact details:

Scott Miller, CEO scott.miller@rampedup.io

Role: Processor

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Subscribers may submit Personal Data to RampedUp Services, the extent of which is determined and controlled by Subscriber in Subscriber's sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Subscriber's prospects, customers, and business partners (who are natural persons)
- Employees or contact persons of Subscriber's prospects, customers, and business partners.
- Subscriber's employees, consultants, contractors, agents and/or third Parties with whom Subscriber conduct s business (who are natural persons)
- Subscriber's Users authorized by Subscriber to use RampedUp Services

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

Subscriber may submit Personal Data to RampedUp Services, the extent of which is determined and controlled by Subscriber in Subscriber's sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Identifiers
- Employment-related information
- Commercial information
- Internet or similar activity

4. SENSITIVE DATA TRANSFERRED

The Parties do not anticipate the transfer of sensitive data under the Agreement.

5. FREQUENCY OF TRANSFER

Data is transferred on a continuous basis depending on Subscriber's use of the RampedUp Services.

6. NATURE OF THE PROCESSING

The nature of the Processing is the provision of the RampedUp Services pursuant to the Agreement.

7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

RampedUp will Process Personal Data as necessary to provide the RampedUp Services pursuant to the Agreement, as further specified in the relevant Documentation, and as further instructed by Subscriber in Subscriber's use of the RampedUp Services.

8. DURATION OF PROCESSING

Subject to Section II (2) of the DPA, RampedUp will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

9. SUB-PROCESSOR TRANSFERS

Sub-processor(s) will Process Personal Data as necessary to provide the RampedUp Services pursuant to the Agreement. Subject to Section III (10) of this DPA, the Sub-processor(s) will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing. Identities of the Sub-processors used for the provision of the RampedUp Services and their country of location are available here: <https://rampedup.io/sub-processors>

10. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland shall act as the competent supervisory authority.

Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as the competent supervisory authority.

Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws

11. TECHNICAL MEASURES

RampedUp manages large-scale contact and company data, and data security is a core priority. We maintain formal, documented information security policies and procedures that are:

- Approved by senior management
- Communicated to staff and available for reference.
- Assigned clear ownership and responsibilities.
- Enforced with disciplinary provisions for non-compliance.
- Reviewed periodically for continued relevance

Employees are required to acknowledge our Code of Conduct and confidentiality obligations, and we maintain a vendor risk assessment program and supporting policies (Information Security Policy, Privacy Policy, Code of Conduct, Incident Response Plan, Data Retention, etc.).

12. INFRASTRUCTURE AND THIRD-PARTY HOSTING

RampedUp is hosted on Amazon Web Services (AWS) and use AWS Key Management Service (KMS) and AES-256 encryption for system backups and key management. RampedUp uses AWS Backup with automatic redundancy restoration to protect against disk failures and maintain data integrity. Programs are monitored regularly (including cost, security, and effectiveness) and maintain a structured third-party / sub-processor review process.

Data protection

- Encryption in transit and at rest
- Data in transit is protected using TLS 1.2.
- Data at rest and backups are encrypted using industry-standard strong encryption, including AES-256 via AWS KMS.

Cryptographic erasure

- When an account expires or is closed, associated data is deleted using cryptographic erasure to ensure it is no longer recoverable.
- Secure deletion & retention
- Admin users have permission to delete data from our service.

- Data provided for specific client relationships is securely deleted or returned at the end of the term using cryptographic erasure.

Data Retention

- Certain datasets are not republished if they have not been refreshed within a defined period (e.g. 15 months).
- RampedUp practices Data minimization, or the principle of collecting, processing, and storing only the minimum amount of personal data that is necessary for a specific, defined purpose.
- At the end of a contract or account lifecycle, data is deleted via cryptographic erasure as described above.

Incident Response

RampedUp has a formal Incident Response Plan, covering preparation, identification, containment, investigation, eradication, recovery, follow-up, and monitoring.

Key practices include:

- Use of AWS services (e.g., CloudTrail, VPC Flow Logs) for logging and monitoring key systems
- Retention of monitoring logs for approximately 30–90 days, with periodic review
- Ability to quickly isolate affected systems (e.g., via security group changes)
- Secure wiping and Key Management Service (KMS)–based cryptographic controls where applicable.

Business Continuity

RampedUp maintains a Business Continuity Management System (BCMS):

- Aligned with ISO 22301 (Business Continuity Management) – aligned but not formally certified.
- Documented Business Continuity Plans (BCP) and Disaster Recovery (DR) procedures are in place and tested periodically.
- AWS documents a series of controls for their hosting infrastructure. Critical data is backed up and available offsite via AWS Backup, with encrypted and redundant storage. Access to hosting facilities is limited, logged, and monitored.

13. SECURITY POLICY AND AWARENESS

The RampedUp IT Security policy undergoes regular reviews to stay aligned with evolving technologies and emerging threats. The policy also requires regular security awareness training, ongoing monitoring of compliance by IT, and notes that non-compliance can lead to loss of access, disciplinary action, or legal consequences.

- Key staff receive security and privacy awareness training, including responsibilities within our BCMS and incident response processes.
- To comply with applicable local privacy laws inside and outside the United States, including EU/UK data protection laws and US state privacy laws such as CCPA/CPRA.

- To maintain a Data Protection Officer (DPO) function and a 23-point vendor risk assessment for key suppliers and sub-processors.

With the exception of information published for public consumption, only formally authorized users may access RampedUp systems, each with a unique user identity. By design, RampedUp employees do not have access to customer passwords. Role-based access control consists of: System Administration, Instance Administration, and User, each with scoped access to customer, partner, or user data to support least-privilege access. Directors responsible for information systems must ensure systems are protected from unauthorized access, secured against theft and damage, used for intended purposes, and that third parties entrusted with data understand and uphold security responsibilities.

Password Policy

RampedUp's Password Policy applies to anyone with access to company systems and data. It requires strong passwords (at least 12 characters with a mix of upper/lowercase, numbers, and special characters), regular password changes every 90 days and prohibits reuse of the last 5 passwords. Passwords must never be stored in plain text, emailed, shared, or written down, and must be kept confidential at all times. After 10 failed login attempts to defend against brute force attacks. Password resets and account recovery must follow secure, verified procedures.