Data Processing Agreement

Insofar as the runZero, Inc. ("**Data Processor**", formerly known as Rumble, Inc.) will be processing personal data on behalf of a data controller ("**Data Controller**") in the course of performing RUNZERO Services, the terms of this Data Processing Agreement ("**DPA**") shall apply. Any capitalized terms not otherwise defined in this DPA shall have the meaning given to them in the Agreement. In the event of a conflict between any provisions of the Agreement for RUNZERO Services (the "**Agreement**") and this DPA, the provisions of this DPA shall govern and control with regard to the processing of personal data. References to "**Data Protection Laws**" shall mean any law applicable to Data Processor's processing or use of personal data, including (to the extent applicable), 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 ("**GDPR**"), and The California Consumer Privacy Act of 2018, AB375, Title 1.81.5, including any implementing law, as amended ("**CCPA**").

1. **Processing**.

a) Data Processor will only process, store, and use the personal data it receives from the Data Controller as necessary to provide the Data Processor's services to the Data Controller, the business purposes as set forth in the Agreement, or Data Controller's prior written instructions. The Data Processor shall never retain, use, disclose, sell, or process the personal data other than as specified in the Data Controller's documented instructions or as otherwise permitted by law.

b) The Data Controller has all necessary rights to provide the personal data to the Data Processor for the processing to be performed in connection with the RUNZERO Services. To the extent required by Data Protection Laws, the Data Controller is responsible for providing all necessary privacy notices to data subjects, and unless another legal basis set forth in the Data Protection Laws supports the lawfulness of the processing, and for obtaining any necessary consents from data subject to the processing required under the Agreement. Should such a consent be revoked by a data subject, the Data Controller will inform the Data Processor of such revocation, and the Data Processor is responsible for implementing Data Controller's instruction with respect to the processing of such personal data.

2. **Confidentiality**.

The Data Processor shall treat all personal data as Confidential Information under the Agreement, and it shall inform all its employees, agents and approved sub-processors engaged in processing the personal data of the confidential nature of the personal data. The Data Processor shall ensure that all such persons or parties have signed confidentiality agreements with obligations no less restrictive in the use and protection of Confidential Information than those in the Agreement.

3. **Security Measures**.

a) Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of personal data appropriate to the risk. The Data Processor shall maintain and follow written security policies that are fully implemented and applicable to the processing of personal data. At a minimum, such policies will include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on permanent staff who will have access to the personal data, conducting appropriate background checks, requiring employees, vendors and others with access to personal data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the personal data aware of information security risks presented by the processing.

b) At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Article 3 and shall allow the Data Controller to audit and test such measures, to the extent it does not require providing access to other customers' data. Subject to such restriction, the Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller, shall grant the Data Controller´s auditors reasonable access to any premises and devices involved with the processing of the personal data, and shall provide the Data Controller´s auditors with access to any information relating to the processing of the personal data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this DPA.

4. **Data Transfers**.

Data Processor may transfer personal data across the border to a country outside of the United States, as necessary to provide the Services. Upon request by the Data Controller, Data Processor will provide details of its transfers of EEA personal data outside of the United States.

Solely to the extent Data Controller transfers any personal data from (a) the European Economic Area, or (b) a jurisdiction where a European Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC is in force and covers such transfer, then the parties agree that such personal data is subject to the model contractual clauses attached hereto as Appendix 1 and annexed to Commission Decision 2004/915/EC (the "**Clauses**"), which are hereby incorporated into the Agreement. In such cases, Data Controller is the 'data exporter' and Data Processor is the 'data importer' as defined in the Clauses.

5. **Security Breach**.

The Data Processor will notify the Data Controller without undue delay upon discovery of any suspected or actual security or confidentiality breach or other compromise of personal data, describing the breach in reasonable detail, the status of any investigation or mitigation taken by the Data Processor, and if applicable, the potential number of data subjects affected. Data Processor will not communicate with any third party regarding any security breach except as specified by other party or by applicable law.

6. **Subprocessors**.

The Data Processor may subcontract any of its RUNZERO Services-related activities or allow any personal data to be processed by a third party, provided that such subprocessors are bound by data protection obligations compatible with those of the Data Processor under this DPA.

7. **Data Subject Rights**.

The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Laws.

RUNZERO, INC.

By: _____________________________________

Name: __________________________________

Title: ___________________________________

CUSTOMER:

By: _____________________________________

Name: __________________________________

Title: ___________________________________

Appendix 1

Standard Contractual Clauses

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(a) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Intentionally Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) 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, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

(f)

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of ________________________.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of ________________________.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 1

This Annex 1 forms part of the Agreement and describes the processing that Data Processor will perform on behalf of Data Controller.

A. List of the Parties

See page 1 of this DPA.

B. Further descriptions of the data processing are provided below:

Scope, nature and purpose of the processing

runZero, Inc. will process the Personal Data for the purposes of providing its Services to the Data Controller in accordance with and as described in the Agreement, the DPA, and these Clauses.

Duration of the processing

The Personal Data will be processed for the term of the Agreement.

Data subjects

The Personal Data to be processed concern the following categories of data subjects:

- Data Controller employees, directors, officers, independent contractors, affiliates, and other individuals who are authorized to use the Services under the Agreement (collectively, "**Users**").

Categories of Personal Data

The Personal Data to be processed concern the following categories of data (please specify):

- Full names

Full names are used by the runZero product to provision authorized users. Full names may also be imported by the platform from third-party data sources (Identity, Directory, MDM, and EDR products, among other options). For users of the public runZero platform (console.runzero.com, console.rumble.run), full names are also imported into company business platforms to enable communication.

- Email addresses

Email addresses are used by the runZero product to provision authorized users. Email addresses may also be imported by the platform from third-party data sources (Identity, Directory, MDM, and EDR products, among other options). For users of the public runZero platform (console.runzero.com, console.rumble.run), email addresses are also imported into company business platforms to enable communication.

- Phone numbers

Phone numbers may be imported by the platform from third-party data sources (Identity, Directory, MDM, and EDR products, among other options). Business phone numbers may be specified in the License information of the runZero product portal. Users that provide a phone number as part of completing marketing and support forms may have this information stored in company business platforms to enable communication.

- Postal addresses

Postal numbers may be imported by the platform from third-party data sources (Identity, Directory, MDM, and EDR products, among other options). Business postal addresses may be specified in the License information of the runZero product portal. Users that provide a postal address as part of completing marketing and support forms will have this information stored in company business platforms to enable communication.

- IP addresses

IP addresses are used in a variety of ways by the runZero platform as well as company business platforms.

The runZero platform provides the ability to scan assets by IP range, resulting in non-personal information about specific IP addresses being stored in the platform. These scanned IP addresses are not directly associated with specific users or personal information. runZero also provides the option to import data from a variety of third-party data sources including but not limited to Identity, Directory, MDM, and EDR products. This imported information may return attributes that associate a company device, personal device, or specific user with an IP address. This information is used to provide an accurate inventory and ownership association for a company-related asset.

The runZero business platforms (web site, CRM, service desk, etc.) may collect and process IP addresses as part of user form submissions, user visits to web content, and form submissions. This IP information may be stored in runZero business platforms and associated with a specific user to support time zone detection, geolocation estimates, and security monitoring.

- MAC addresses

MAC addresses are used by the runZero platform to associate non-personal information with specific devices. Unauthenticated network scans may collect and associate a MAC address with specific assets in order to determine the manufacture, age, and unique network identifier of that asset. runZero also provides the option to import data from a variety of third-party data sources including but not limited to Identity, Directory, MDM, and EDR products. This imported information may return attributes that associate a company device, personal device, or specific user with a MAC address. This information is used to provide an accurate inventory and ownership association for a company-related asset.

Special categories of Personal Data (if applicable): None

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

Continuous, or as the Services are used.

Nature of the processing

Collection, organization, storage, use, disclosure, erasure, augmentation, enrichment, transmission.

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

Upon the termination or expiration of the Agreement, or at any time upon Data Controller's request, Data Processor will immediately cease to process Data Controller Data and will promptly return or destroy the Data Controller Data (including all copies) in Data Processor's possession or control (including any Data Controller Data held by Subprocessors) as instructed by Data Controller. Data stored in operational backups will be maintained based on the Data Processor's backup retention policy.

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

Please refer to Annex III

C. Competent Supervisory Authority

In accordance with Clause 13, the competent Supervisory Authority is: the supervisory authority for the Member State in which Data Controller is established.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

runZero is committed to implementing appropriate technical and organizational security measures to meet its obligations. runZero has internally documented policies and controls designed to ensure the security of customer and internal data. These policies refer to all data collected from employees, candidates, users, customers, vendors, or other parties that provide information to us. runZero employees must follow these policies. Contractors, consultants, partners and any other external entities are also covered. Generally, these policies include anyone we collaborate with or who acts on our behalf and may need access to data.

To help comply with these policies and controls, we will:

- Classify all data and apply appropriate controls for each level
- Employ encryption of all customer data in transit and at rest to minimum industry standards
- Perform periodic reviews of all our security policies and controls
- Schedule annual penetration tests of the platform and remediate appropriately
- Perform annualized security training for all runZero employees
- Utilize centralized monitoring and logging of all runZero production systems

ANNEX III

LIST OF SUBPROCESSORS

Last updated: 2022-12-20
Last subprocessor addition: 2022-11-30
Last subprocessor removal: 2022-11-30

Please note that each subprocessor also references a list of scopes where personal data may be sourced from. The definition of each of these scopes is below:

- runZero Websites: The primary www.runzero.com website as well as related domains and subdomains that are managed by the runZero team, excluding the runZero platform itself.
- runZero Public Cloud: The console.runzero.com and console.rumble.run application portals hosted within the AWS platform. This is the default environment for new accounts unless provisioned separately.
- runZero Private Clouds: Customer-specific cloud environments hosted by runZero within the AWS platform. These environments are logically and/or physically separated from the public cloud.
- runZero Self-Hosted: Customer-hosted installations of the runZero platform. Self-hosted customers also have access to the runZero Public Cloud to access downloads and license updates. Only a single user record is required in the Public Cloud to access the self-hosted resources.
- Manual: A system used by runZero staff to provide services and manage the business.

Subprocessor	**Services Provided**	**Location**	**Types of Personal Data**	**Platforms in Scope**	**If Applicable, Adequacy Mechanism Supporting Transfer of Amazon Personal Information Originating in the European Economic Area and/or Switzerland (e.g., EU Standard Contractual Clauses, Binding Corporate Rules, etc.)**
6Sense Insights, Inc. (including Slintel)	Sales and marketing analytics	USA	Name, email address, phone number, postal address, and IP address	runZero Websites	EU Standard Contractual Clauses
A-LIGN Compliance and Security, Inc.,	SOC 2 support and auditing	USA	Business contact information (name, email) as	runZero Websites runZero Public Cloud runZero Private Clouds	EU Standard Contractual Clauses

d/b/a A-LIGN			relevant to SOC2 compliance and auditing.		
Amazon Web Services, Inc.	Infrastructure (IaaS)	USA	Name, email address, phone number, postal address, IP address, and MAC address. AWS is our primary IaaS provider.	runZero Websites runZero Public Cloud runZero Private Clouds Manual	EU Standard Contractual Clauses
Avalara, Inc.	Sales tax management	USA	Business contact information (name, email) as relevant to accounting and tax reporting.	runZero Public Cloud Manual	EU Standard Contractual Clauses
Bill.com, LLC	Payment processing	USA	Business contact information (name, email) as relevant to accounting and accounts payable.	Manual	EU Standard Contractual Clauses
ByteChek, Inc.	SOC 2 support and auditing	USA	Limited visibility into AWS infrastructure, but without access to personal information or platform data.	runZero Websites runZero Public Cloud runZero Private Clouds	EU Standard Contractual Clauses
Digital Ocean, Inc.	Infrastructure (IaaS) and Hosted External Scans	USA	IP addresses of internet-facing assets (non-personal). This provider is only used when Hosted Scans are run from the runZero platform.	runZero Public Cloud runZero Private Clouds	EU Standard Contractual Clauses
Docebo NA, Inc.	Training, certification, and support content	USA	Business contact information (name, email) as relevant to user	Manual	EU Standard Contractual Clauses

			enrollment in training courses. Docebo use is optional and separate from the runZero websites and platform.		
Drata, Inc.	SOC 2 support	USA	Limited visibility into AWS infrastructure, but without access to personal information or platform data.	runZero Websites runZero Public Cloud runZero Private Clouds Manual	EU Standard Contractual Clauses
Formagrid Inc. d/b/a Airtable	Project management	USA	Business contact information (name, email) as relevant to project tracking.	Manual	EU Standard Contractual Clauses
Freshworks Inc.	Technical support ticketing	USA	Business contact information (name, email) in addition to any information shared as part of a support case. Tickets are created in Freshworks when submitted from the runZero Website or the runZero Public Cloud/Private Cloud in-product Support forms. Customers may also open a case by emailing support@runzero.com, which is the primary support mechanism for self-hosted customers.	runZero Websites runZero Public Cloud runZero Private Clouds Manual	EU Standard Contractual Clauses
General Outline,	Wiki / intranet	USA	Business contact	Manual	EU Standard Contractual

Inc. d/b/a Outline			information (name, email) as relevant to project tracking.		Clauses
GitHub, Inc.	Source code repository, ticketing, project tracking	USA	Business contact (name, email) information as well as specific asset information when the “Improve Fingerprint” option is used within the runZero Public Cloud and runZero Private Cloud product. The specific asset information may include IP addresses and MAC addresses of that asset.	runZero Public Cloud runZero Private Clouds Manual	EU Standard Contractual Clauses
Google LLC	Email, storage, office packages, analytics, advertising	USA	Business contact information (name, email, phone number, postal address). Google Workspace is runZero’s email and identity provider. runZero website and platform events can generate email that is routed to Google Workspace as part of business workflows (creating a service ticket, notifying the operations team, etc).	runZero Websites runZero Public Cloud runZero Private Clouds Manual	EU Standard Contractual Clauses
HubSpot, Inc.	Sales and marketing	USA	Business contact information	runZero Websites runZero Public Cloud	EU Standard Contractual Clauses

	automation, analytics		(name, email, phone number, postal address). HubSpot is our primary CRM, sales, and marketing operations platform. The runZero Public Cloud/Private Clouds also report non-personal analytics information to HubSpot to enable business communication (license use, feature utilization, etc.).	runZero Private Clouds Manual	
Impartner, Inc., formally known as Treehouse Interactive, Inc	Partner enablement, training, and performance tracking	USA	Business contact information (name, email, phone number, postal address).	runZero Websites Manual	EU Standard Contractual Clauses
Celonis, Inc (as make.com: formerly Integromat s.r.o.)	Sales and marketing orchestration	USA	Business contact information (name, email, phone number, postal address).	Manual	EU Standard Contractual Clauses
Intuit Inc.	Bookkeeping, accounting	USA	Business contact information (name, email, phone number, postal address) as relevant to accounting.	runZero Public Cloud Manual	EU Standard Contractual Clauses
JN PROJECTS Inc. d/b/a HelloSign	Digital document signatures and management	USA	Business contact information (name email). HelloSign is used for document signing as needed for specific business	Manual	EU Standard Contractual Clauses

			agreements.		
LinkedIn Corporation	Sales and recruiting technology	USA	LinkedIn is used to reach out to customers and prospects as part of business communication. Customer information is not imported into LinkedIn, but existing LinkedIn profile information is used for communication.	Manual	EU Standard Contractual Clauses
SO Holdco, LLC dba Maxio (SaaS Optics, Chargify, Keen)	Finance operations, e-commerce, customer billing, and account management	USA	Business contact information (name, email, phone number, postal address) as relevant to accounting and e-commerce processing.	runZero Public Cloud Manual	EU Standard Contractual Clauses
Objectis Ltd. d/b/a Cookie-Script	Consent management platform	European Union (Lithuania)	IP address is used for automatic location detection as part of cookie consent processing.	runZero Websites	EU Standard Contractual Clauses
Plausible Insights OÜ	Marketing analytics	European Union (Estonia)	IP addresses are collected, but not saved, as part of this privacy-friendly analytics platform.	runZero Websites	EU Standard Contractual Clauses
QuotaPath, Inc.	Sales performance tracking	USA	Business contact information (name, email, phone number, postal address) as relevant to accounting and sales tracking.	Manual	EU Standard Contractual Clauses

Reclaim.ai, Inc.	Calendaring	USA	Business contact information (name, email, phone number) as necessary for meeting invitations.	runZero Websites Manual	EU Standard Contractual Clauses
Seamless Contacts, Inc.	Marketing database augmentation	USA	Business contact information (name, email, phone number). Seamless augments existing contact records used for business communication.	Manual	EU Standard Contractual Clauses
Slack Technologies, LLC	Internal and customer communication	USA	Business contact information (name, email) for specific email aliases routed to Slack channels. Customer contact information may be shared in Slack as part of support and sales coordination. Limited platform information may be shown in Slack when related to a system alert or other health monitoring task. Live chat from the runZero websites may also be shared in Slack channels.	runZero Websites runZero Public Cloud runZero Private Clouds Manual	EU Standard Contractual Clauses
Stripe, Inc. (including TaxJar)	Payment processing, tax calculation, invoicing, subscription	USA	Business contact information (name, email, phone number, postal address) as	runZero Public Cloud Manual	EU Standard Contractual Clauses

	management		relevant to accounting and e-commerce purchase and subscription processing. IP addresses may be processed as well as part of fraud controls and security monitoring.		
Zoom Video Communications, Inc.	Video conferencing (internal and with customers)	USA	Business contact information (name, email, phone number) as part of scheduling video conference calls.	Manual	EU Standard Contractual Clauses

[Remainder of page intentionally left blank]