**Data Processing Agreement**

This Data Processing Agreement (“Agreement”) dated [DATE] (the “Effective Date”) between: Fundraise Up Inc., a Delaware corporation with a place of business at 114 8th Street, Brooklyn, New York 11215 USA (“Vendor”) acting on its own behalf and as agent for its Affiliates, and [COMPANY], a [STATE/COUNTRY] [TYPE OF COMPANY] with a place of business at [ADDRESS] (“Company”) acting on its own behalf and as agent for its Affiliates.

1. Definitions
   1. The definitions of this Section 1.1 shall apply to this Agreement, and cognate terms shall be construed accordingly.
      1. “Affiliate” means any entity which 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.
      2. “Applicable Laws” means any United States, United Kingdom, European Union (“EU”), Member State, or the data protection or privacy laws of any other country, that apply to any Company Personal Data and to which any Contracted Vendor or Company Group Member is subject.
      3. “Company Group Member” means Company or any Company Affiliate.
      4. “Company Personal Data” means any Personal Data Processed by a Contracted Vendor on behalf of a Company Group Member pursuant to this Agreement.
      5. “Contracted Vendor” means Vendor, a sub-contractor, a Subprocessor, or Affiliates thereof.
      6. “Data Subject” means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to Personal Data, and who is resident in a country, state, or other region to which one or more Applicable Laws apply.
      7. “EEA” means the European Economic Area.
      8. “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
      9. “GDPR” means, as applicable, the EU General Data Protection Regulation 2016/679 (“EU GDPR”), including, as retained by the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018, and as amended (“UK GDPR”).
      10. “Personal Data” means generally personal data and/or personal information as defined under Applicable Laws including, but not limited to, ‘personal data’ as defined under the GDPR. Personal Data excludes publicly available, anonymous, pseudonymous (provided the key to re-identifying any Data Subject is kept separate and secure), de-identified, statistical, and/or aggregate information.
      11. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, exfiltration or theft of, Personal Data transmitted, stored, or otherwise Processed.
      12. “Processing” or any variation thereof, including cognate forms, with respect to data means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, including, but not limited to collection, recording, organization, disclosure by transmission, storage, dissemination or otherwise making available, retrieval, use, erasure, or destruction.
      13. “Restricted Transfer” means:
          1. a transfer of Company Personal Data from any Company Group Member to a Contracted Vendor; or
          2. any onward transfer of Company Personal Data from any Contracted Vendor to another Contracted Vendor, or between two facilities of a Contracted Vendor;

in each case, where such transfer would be prohibited by Applicable Laws in the absence of appropriate safeguards, as required by GDPR Article 46, including without limitation, Standard Contractual Clauses, binding corporate rules, or other approved mechanisms (“Appropriate Safeguard”).

* + 1. “Services” means the services and other activities to be provided by a Contracted Vendor for a Company Group Member.
    2. “Standard Contractual Clauses” means the contractual clauses set out by Commission Decision (EU) 2021/914.
    3. “Subprocessor” means any person (including any third party and any Vendor Affiliate, or sub-contractor, but excluding employees of Vendor or its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with this Agreement.
  1. The terms, “Commission,” “Controller,” “Member State,” “Processor,” and “Supervisory Authority” shall have the meanings assigned in the EU Data Protection Laws.
  2. The word “include” shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

1. Status of the Parties.

For the purposes of this Agreement, the Vendor shall be a Processor and Company shall be a Controller.

1. Processing of Company Personal Data.
   1. Each Contracted Vendor shall:
      1. comply with all Applicable Laws in the Processing of Company Personal Data;
      2. if required by GDPR Article 30, maintain a record of all Processing activities carried out on Company Personal Data; and
      3. only Process Company Personal Data as instructed by the relevant Company Group Member, unless such Processing is required by Applicable Laws in which case the Contracted Vendor shall inform the Company Group Member of that legal requirement (to the extent permitted by the Applicable Laws) before Processing that Company Personal Data, or unless such instruction is, in the Contracted Vendor’s good faith belief, violative of Applicable Laws, in which case the Contracted Vendor will immediately notify Company that it is unable to comply with said instruction.
   2. Each Company Group Member hereby:
      1. instructs Contracted Vendor, only as necessary to provide, and in furtherance of, the Services, to:
         1. Process Company Personal Data; and
         2. transfer Company Personal Data to any country or territory,

provided that, if necessary, an Appropriate Safeguard is in place before any such transfer takes place;

* + 1. agrees that it shall, at all times relevant to this Agreement, comply with all Applicable Laws;
    2. represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in Section 3.2.1 on behalf of each relevant Company Affiliate; and
    3. represents and warrants that it will determine an appropriate legal basis, or bases, for the Processing of Company Personal Data which is necessary to perform the Services, and will upon request by Vendor provide proof of the legal basis/bases for processing, as well as compliance with Applicable Laws.
  1. Pursuant to GDPR Article 28(3), Company agrees that the descriptions of i) the subject matter, duration, nature and purpose of Processing, ii) the types of Company Personal Data to be Processed, and iii) the categories of Data Subjects within the Company Personal Data to be Processed under this Agreement, are sufficiently specified in the Contracted Vendor’s technical documentation as received by Company and within Annex 1, attached to this Agreement. Company will notify the Contracted Vendor with respect to any revisions to such descriptions that may be required regarding the Company Personal Data. Upon written notice to Company, the Vendor may make reasonable revisions to such descriptions from time to time in order to maintain compliance with Applicable Laws.

1. Contracted Vendor Personnel.

Each Contracted Vendor shall ensure the reliability of any employee, agent or contractor of such Contracted Vendor who may have access to the Company Personal Data; and ensure in each case that access is strictly limited to those individuals that have a need to know or access the relevant Company Personal Data to perform the Services hereunder, who are obligated to keep such Company Personal Data confidential, and to comply with Applicable Laws in the context of that individual's duties.

1. Security.
   1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks (of varying likelihood and severity) to the rights and freedoms of natural persons, each Contracted Vendor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to those risks, including, as appropriate, the security measures referred to in GDPR Article 32(1) (e.g., pseudonymization and encryption).
   2. In assessing the appropriate level of security provided under Section 5.1, each Contracted Vendor shall take into account the risks that arise from their respective Processing of Company Personal Data, including Personal Data Breaches
   3. In the event that the Vendor receives a request from a government agency or law enforcement authority to produce, or provide it with access to, Company Personal Data, it shall:
      1. Notify Company of such request to the extent that it is legally permitted to do so;
      2. Make a good faith effort to determine if such request is legally enforceable; and
      3. Disclose only the minimum necessary to comply with such request if such request is legally enforceable.
2. Subprocessing.
   1. Each Company Group Member: i) approves Vendor’s and each Vendor Affiliate’s current Subprocessors; and ii) authorizes Vendor and each Vendor Affiliate to appoint (and permit authorized Subprocessors to appoint) new Subprocessors in accordance with this Section 6.
   2. Vendor and any applicable Vendor Affiliate shall give Company, if it subscribes, prior written notice before appointing any new Subprocessor, including details of the Processing to be undertaken by the Subprocessor. Company must subscribe to receive such notices by emailing [legal@fundraiseup.com](mailto:legal@fundraiseup.com) with “Subscribe” in the subject line and providing sufficient detail so as to identify this Agreement. If, within fifteen (15) days of receipt of such notice, Company notifies Vendor in writing of any reasonable objections to the proposed appointment, then neither Vendor nor any Vendor Affiliate shall appoint, or disclose any Company Personal Data to, such proposed Subprocessor. Vendor or the applicable Vendor Affiliate may then develop and disclose to Company a written plan to address the objections raised by Company. If Company accepts such plan in writing, then Vendor or the applicable Vendor Affiliate may proceed to appoint the proposed Subprocessor. If Company reasonably objects to such plan as insufficient, the parties shall work together in good faith to either adjust the plan, or effect a commercially reasonable change in the provision of the Services that avoids the use of that proposed Subprocessor. If the forgoing change in the provision of the Services is not commercially reasonable as agreed by the parties, either party may terminate this Agreement upon written notice to the other party.
   3. With respect to each Subprocessor, the Vendor or relevant Vendor Affiliate shall:
      1. ensure that the Subcontractor is bound by a written agreement that offers terms at least as restrictive as those set out in this Agreement, and meets the requirements of Article 28(3) of the GDPR (“Subprocessor Agreement”);
      2. ensure that an Appropriate Safeguard is in place with any Subprocessor prior to any contemplated Restricted Transfers; or ensure that Subprocessor enters into an agreement with the relevant Company Group Member(s) incorporating the Standard Contractual Clauses (and Company shall ensure that each relevant Company Affiliate executes such Standard Contractual Clauses) before the Subprocessor may Process Company Personal Data; and
      3. provide copies of the Subprocessor Agreement to Company for review (which copies may be redacted to remove confidential information not relevant to the requirements of this Agreement) as Company may request from time to time.
   4. Vendor shall remain responsible for its compliance with the obligations of this Agreement and for any acts or omissions of its Subprocessors that cause Vendor to breach any of its obligations under this Agreement.
3. Data Subject Rights.
   1. Taking into account the nature of the Processing, each Contracted Vendor shall reasonably support each Company Group Member in implementing appropriate, and commercially reasonable, technical and organizational measures for the purpose of fulfilling Company Group Members' obligations to respond to requests to exercise Data Subject rights under the Applicable Laws.
   2. Vendor shall:
      1. promptly notify Company if any Contracted Vendor receives a request from a Data Subject under any Applicable Laws with respect to Company Personal Data; and
      2. ensure that the Contracted Vendor does not respond to that request except: i) as agreed by the Vendor and the Company; or ii) as required by Applicable Laws to which the Contracted Vendor is subject, in which case Vendor shall (to the extent permitted by Applicable Laws) inform Company of that legal requirement before the Contracted Vendor responds to the request.
4. Personal Data Breach.

Vendor shall, without undue delay, notify Company upon becoming aware that any Contracted Vendor experienced Personal Data Breach affecting Company Personal Data, and provide Company with a primary point of contact at the Contracted Vendor and sufficient information to allow each Company Group Member to meet any obligations to report or inform the applicable Data Subjects and/or Supervisory Authorities of the Personal Data Breach under the Applicable Laws. Such information may be provided in phases if it is impossible or impractical to provide simultaneously.

1. Data Protection Impact Assessment and Prior Consultation.

Each applicable Contracted Vendor shall provide reasonable assistance to each Company Group Member in performing any data protection impact assessments and/or relevant consultations with Supervisory Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by GDPR Articles 35 or 36, or equivalent provisions of any other Applicable Laws, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Vendor. Any such assistance provided by a Contracted Vendor to a Company Group Member shall be at Company’s sole cost and expense.

1. Deletion or Return of Company Personal Data.
   1. Subject to Sections 10.2 and 10.3, each applicable Contracted Vendor shall within thirty (30) days after the date of cessation of Services involving the Processing of Company Personal Data (the “Cessation Date”), delete and ensure the deletion of all copies of those Company Personal Data.
   2. Subject to Section 10.3, Company may by written notice to Vendor within thirty (30) days of said notice require each applicable Contracted Vendor to (a) return a complete copy of all Company Personal Data in such Contracted Vendor’s possession, or under its control, to Company by secure file transfer in any common digital format; and (b) delete and ensure the deletion of all copies of Company Personal Data Processed by any Contracted Vendor in such Contracted Vendor’s possession, or under its control.
   3. Notwithstanding anything to the contrary in 10.1 and 10.2, each Contracted Vendor may retain Company Personal Data to the extent and for such period as is required by Applicable Laws, provided that such Contracted Vendor shall ensure the confidentiality of all such retained Company Personal Data, and shall ensure that the Company Personal Data are only retained only for the purpose(s) specified in the Applicable Laws requiring its retention. For the avoidance of doubt, the terms and conditions of this Agreement shall continue to apply to such retained Company Personal Data for so long as it is retained by such Contracted Vendor.
2. Audit Rights.
   1. Subject to Section 11.2, each applicable Contracted Vendor shall reasonably make available to each Company Group Member on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and cooperate with audits, including inspections, by any Company Group Member or an auditor appointed by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Vendor.
   2. The applicable Company Group Member undertaking an audit shall give at least fifteen (15) days’ written notice to the applicable Contracted Vendor with regard to any audit or inspection to be conducted under Section 11.1, and shall reasonably avoid (and ensure that each of its appointed auditors reasonably avoids) causing any damage, injury or disruption to the Contracted Vendor's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection:
   3. A Contracted Vendor need not give access to its premises for the purposes of an audit or inspection under Section 11.1:
      1. to any individual unless he or she produces reasonable evidence of identity and authority;
      2. without the person or entity conducting the audit binding itself in writing to terms of confidentiality acceptable to Vendor;
      3. outside normal business hours; or
      4. more than once per year.
   4. In the event that an audit reveals the Contracted Vendor is not in compliance with the terms and conditions of this Agreement or Applicable Laws, the Company Group Member will promptly notify the Contracted Vendor of such non-compliance. The Vendor and/or Contracted Vendor agree(s) that such non-compliance shall be materially remedied within thirty (30) days of its receipt of notice of non-compliance, and if it does not, Vendor and/or Contracted Vendor further agrees that Company and/or applicable Company Group Member may immediately upon notice to Vendor, terminate this Agreement.
   5. Any audit or inspection conducted under this Section 11 shall be at Company’s sole cost and expense and Company shall indemnify, defend and hold harmless Contracted Vendor from any act or omission of any employee, agent or representative of Company or a mandated third-party auditor during such audit or inspection.
3. Restricted Transfers.
   1. With respect to Restricted Transfers taking place between the Company Group Member and the Vendor, if applicable, the Company Group Member shall encrypt the Company Personal Data prior to transferring it to the Vendor, and the Appropriate Safeguard shall be as provided in Annex 2 for Personal Data subject to the EU GDPR, and in the case of Personal Data subject to the UK GDPR the Appropriate Safeguard shall comprise Annex 2 and Annex 3 together, as applicable to this Agreement. After careful consideration by the parties of the circumstances of such Restricted Transfer to the United States, the applicable Appropriate Safeguard described above, and the additional safeguards provided in this Agreement, provide the Data Subjects who are located in the EEA and whose Personal Data is Processed hereunder enjoy an essentially equivalent level of protection and rights as they do under the EU GDPR in the EEA with respect to their Personal Data (“Essential Equivalence”).
   2. Before it commences any Restricted Transfer to a Subprocessor, a Contracted Vendor shall ensure that an Appropriate Safeguard exists between itself and the Subprocessor, or if necessary, between the Company Group Member (the “Data Exporter”) and the Subprocessor (the “Data Importer”) that provides Essential Equivalence for applicable Data Subjects, and if that is not the case, the Contracted Vendor shall institute such additional safeguards as are necessary to provide Essential Equivalence in the country that the Company Personal Data will be imported into.
   3. Notwithstanding anything to the contrary herein, for sole purpose of engaging in Restricted Transfers, which are strictly necessary to perform the Services under this Agreement, and only where the Standard Contractual Clauses are the Appropriate Safeguard selected, Company Group Member grants to the Contracted Vendor limited agency rights to enter into the Standard Contractual Clauses on its behalf with the applicable Vendor Affiliate or Subprocessor.
4. Term and Termination. This Agreement shall be effective from the Effective Date until the Services are completed, or the earlier termination of this Agreement by either party as set forth herein. This Agreement may be terminated for cause upon thirty (30) calendar days’ notice if the other party breaches a material term of this Agreement, and such breach is not materially cured within thirty (30) calendar days. Additionally, Vendor may terminate this Agreement with or without cause upon ten (10) days’ notice to Company without penalty, liability, or further obligation. Termination will not affect any part of this Agreement which is explicitly indicated to survive, or by its nature survives, the termination of this Agreement.
5. Indemnification. Company agrees to defend, indemnify, and hold harmless Vendor and all Contracted Vendors and their respective directors, officers, employees, and agents from and against all damages, costs (including reasonable attorneys’ fees), judgments and other expenses arising out of or on account of a third-party lawsuit, investigation, allegation, proceeding or other claim arising from or relating to (i) the performance of the Services by any Contracted Vendor that were directed by a Company Group Member; (ii) any actual or alleged breach of this Agreement or applicable law by any Company Group Member(s); and (iii) the acts and omissions of Company Group Members.
6. Limitations.
   1. Damages. EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, VENDOR SHALL NOT BE LIABLE TO COMPANY FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND OR NATURE, INCLUDING, WITHOUT LIMITATION, DAMAGES ARISING FROM THE BREACH OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, EVEN IF VENDOR HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH LOSS OR DAMAGE.
   2. Liability. EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, VENDOR’S MAXIMUM AND TOTAL LIABILITY ARISING FROM OR IN CONNECTION WITH THIS AGREEMENT SHALL NOT EXCEED THE TOTAL OF THE AMOUNTS ACTUALLY PAID BY COMPANY TO VENDOR IN CONNECTION WITH THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PROCEEDING THE EVENT GIVING RISE TO SUCH LIABILITY.
7. General Terms.
   1. Governing Law and Jurisdiction; Arbitration.
      1. The laws of the EU Member State in which the Company is established, or, if the Company is not established in the EU, the laws of the State of New York, USA, shall govern the validity, construction, performance, and enforcement of this Agreement without giving effect to the principle of conflict of laws.
      2. Arbitration. Each party agrees to submit any and all disputes, claims and controversies arising between the parties hereto to final and binding arbitration, which shall be administered by the American Arbitration Association (“AAA”) in accordance with its rules then in effect, including with respect to the payment of all filing, administration and arbitrator fees. Any arbitration brought hereunder shall be heard by three (3) independent and impartial arbitrators. Two arbitrators shall be selected by the respective parties, one by the claimant(s) and one by the respondent(s). The third arbitrator shall be appointed by the two party-appointed arbitrators or by the AAA if such two arbitrators cannot agree. The place of the arbitration shall be New York, New York. Such Arbitration shall take place in English. Any party’s refusal to select, or unreasonable delay in selecting, an arbitrator shall be considered a material breach of this Agreement. The arbitrators shall have the authority to grant any equitable and legal remedies that would be available in any judicial proceeding intended to resolve a dispute. Notwithstanding the foregoing, either party shall be entitled to bring an action seeking injunctive relief in any court of competent jurisdiction. The award rendered in an arbitration hereunder shall be final and non-appealable. Judgment on the award rendered may be entered in any court having jurisdiction thereof. Each of the parties shall keep the proceedings and any and all transcripts, statements, documents, discovery, correspondence and all other non-public information produced or otherwise disclosed in connection with any such arbitration confidential.
      3. To the extent arbitration does not apply, Company agrees that any dispute arising out of or relating to the Service, or to Vendor, may only be brought by Company in a state or federal court located in New York City, New York. EACH PARTY HEREBY WAIVES ANY OBJECTION TO THIS VENUE AS INCONVENIENT OR INAPPROPRIATE, AND AGREE TO EXCLUSIVE JURISDICTION AND VENUE IN NEW YORK.
   2. Precedence. In the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties (except where explicitly agreed otherwise in writing by the parties), the provisions of this Agreement shall prevail with respect to the subject matter herein.
   3. Independent Contractors. Except with respect to the limited exception provided in Section 12.3 above, it is expressly agreed that the parties shall be independent contractors and that the relationship between the parties shall not constitute a partnership, joint venture, or agency. Neither party shall have the authority to make any statements, representations or commitments of any kind, or to take any action, which shall be binding on the other party, without the prior consent of such other party.
   4. Either party may upon at least thirty (30) days' written notice to the other party:
      1. terminate the use of a given Appropriate Safeguard, to the extent required by any change in, or decision of a competent authority under, the Applicable Laws in favor of another Appropriate Safeguard for making Restricted Transfers, and the notified party hereby agrees that it will execute such documents or agreements as may be reasonably necessary to do so, and to reasonably assist the notifying party in perfecting the same Appropriate Safeguards with any of its Subprocessors, if applicable; and
      2. propose any other variations to this Agreement that the notifying party reasonably considers to be necessary to address the requirements of any Applicable Laws. The parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.
   5. If Company gives notice under Section 16.4.1:
      1. the Contracted Vendor shall reasonably co-operate (and ensure that any affected Subprocessors promptly co-operate, if applicable) to ensure that equivalent variations are made to any agreement put in place under Section 6.3.2; and
      2. Company shall not unreasonably withhold, condition, or delay agreement to any variations to this Agreement proposed by Vendor to protect the Contracted Vendor against additional risks associated with the variations made under Section 16.4.1 and/or 16.4.2.
   6. Notice. For purposes of all formal notices required to be given hereunder, the addresses of the parties hereto shall be as indicated below. All notices shall be in writing and shall be deemed to have been duly given on the date received if sent by first class registered or certified mail or its equivalent, return receipt requested, or overnight delivery service. All notices shall be addressed to the attention of the signatories of parties below at their respective addresses as first set forth above.
   7. Severability. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to make it valid and enforceable, while preserving the parties’ intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.
   8. Assignment. Except as otherwise expressly permitted in this Agreement, neither party may sell, transfer, or assign its rights and duties under this Agreement without the prior written consent of the other party. Any impermissible assignment or transfer shall be null and void. Notwithstanding the foregoing, either party may assign its duties and obligations under this Agreement in connection with an acquisition, merger, reorganization, recapitalization or a sale of substantially all of its assets. This Agreement shall inure to the benefit of the parties, their successors and permitted assigns.
   9. Waiver.No waiver shall be effective unless consented to by both parties in writing. No failure or delay by either party in exercising any rights, powers, or remedies under this Agreement shall operate as a waiver of any such right, power, or remedy.
   10. Entire Agreement. This Agreement and all of its appendices and exhibits, all of which are incorporated herein by reference, contains the entire understanding and agreement of the parties with respect to the subject matter contained herein. This Agreement supersedes all prior oral or written understandings and agreements relating thereto except as expressly otherwise provided, and may not be altered, modified or waived in whole or in part, except in writing, signed by duly authorized representatives of the parties. The parties shall not require the consent or approval of any Company Affiliate or another Contracted Vendor to amend this Agreement.
   11. Counterparts. This Agreement may be executed counterparts, by facsimile, electronic signature, scanned signature or otherwise, each of which shall be deemed to be an original, but all of which, together, shall constitute one and the same instrument.

[*Signatures on following page*]

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding upon the parties as of the Effective Date.

**FUNDRAISE UP INC.**

By:

Print Name: Yuriy Smirnov

Title: Chief Technology Officer

By:

Print Name:

Title:

**ANNEX 1**

**TO THE DATA PROCESSING AGREEMENT**

This Annex forms part of the Agreement as agreed by the parties.

1. Subject Matter of Processing: Vendor’s provision of Services to the Company.
2. Categories of Data Subjects.
   1. Individuals making donations to the Company, and individuals that work for the Company.
3. Categories of Personal Data.
   1. Name, email address, location, name of employer, truncated payment card number, payment card CVC code, and IP address.
4. Special Categories of Data (if appropriate).
   1. No special data collected, received or processed.
5. Processing operations and duration. The Personal Data transferred will be subject to the following basic Processing activities: managing an e-commerce platform for charitable organizations. Such Processing activities shall continue for the term of the provision of Services and for any amount of time thereafter which Company Personal Data is retained.

**ANNEX 2**

**STANDARD CONTRACTUAL CLAUSES**

**SECTION I**

*Clause 1*

***Purpose and scope***

* 1. 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.
  2. The Parties:
     + 1. 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
       2. 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”).

* 1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
  2. 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***

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.

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***

* 1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
     + 1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
       2. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
       3. Clause 9 - Clause 9(a), (c), (d) and (e);
       4. Clause 12 - Clause 12(a), (d) and (f);
       5. Clause 13;
       6. Clause 15.1(c), (d) and (e);
       7. Clause 16(e); and
       8. Clause 18 - Clause 18(a) and (b);
  2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

* 1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
  2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
  3. 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 - Optional*

***Docking clause***

* 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
  2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
  3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**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**

* 1. 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.
  2. 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**

* 1. 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.
  2. 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.
  3. 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.
  4. 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:

* + - 1. 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;
      2. 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;
      3. 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
      4. 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**

* 1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
  2. 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.
  3. 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.
  4. 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.
  5. 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***

* 1. 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 fifteen (15) 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.
  2. 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.
  3. 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.
  4. 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.
  5. 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***

* 1. 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.
  2. 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.
  3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*

***Redress***

* 1. 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.
  2. 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.
  3. 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:
     + 1. 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;
       2. refer the dispute to the competent courts within the meaning of Clause 18.
  4. 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.
  5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
  6. 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***

* 1. 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.
  2. 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.
  3. 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.
  4. 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.
  5. 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.
  6. 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.
  7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

* 1. The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
  2. 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***

* 1. 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.
  2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
     + 1. 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;
       2. 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;
       3. 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.
  3. 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.
  4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
  5. 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).
  6. 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**

* 1. 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:
     + 1. 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
       2. 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.
  2. 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.
  3. 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.).
  4. 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.
  5. 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**

* 1. 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).
  2. 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.
  3. 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***

* 1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
  2. 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).
  3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
     + 1. 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;
       2. the data importer is in substantial or persistent breach of these Clauses; or
       3. 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.

* 1. 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.
  2. 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.

*Clause 17*

***Governing law***

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France (*specify Member State*).

*Clause 18*

***Choice of forum and jurisdiction***

* 1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
  2. The Parties agree that those shall be the courts of the Member State indicated in Clause 17.
  3. 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.
  4. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role: … Controller

[2. … Name: … Fundraise Up Inc.

Address: …114 8th Street, Brooklyn, New York 11215 USA

Contact person’s name, position and contact details: … Yuriy Smirnov, Chief Technology Officer, (718) 599-1129, [legal@fundraiseup.com](mailto:legal@fundraiseup.com)

Activities relevant to the data transferred under these Clauses: … managing an e-commerce platform for charitable organizations.

Signature and date: …

Role: …Processor

EU Representative: Brown Rudnick

1 rue François 1er

75008 Paris

France]

**Data importer(s):**

1. Name: … Fundraise Up Inc.

Address: …114 8th Street, Brooklyn, New York 11215 USA

Contact person’s name, position and contact details: … Yuriy Smirnov, Chief Technology Officer, (718) 599-1129, [legal@fundraiseup.com](mailto:legal@fundraiseup.com)

Activities relevant to the data transferred under these Clauses: … managing an e-commerce platform for charitable organizations.

Signature and date: …

Role: …Processor

EU Representative: Brown Rudnick

1 rue François 1er

75008 Paris

France

2. …[*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role: … Controller]

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

*Individuals making donations to the Company, and individuals that work for the Company.Categories of personal data transferred.*

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

*No sensitive data collected, received or processed.*

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

*Continuous*

*Nature of the processing*

*Receive, collect, store, use, adapt and retrieve the data.*

*Purpose(s) of the data transfer and further processing*

*To allow Vendor to provide services to Compan.*

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

*For the term of the provision of Vendor’s services to Company.*

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

*……………………..*

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*Commission nationale de l'informatique et des libertés.*

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Secure socket layer level encryption; least privilege access; access control list and log; strictly enforced password policies; annual third party audit of security measures; and the entire network on which the e-commerce platform exists on a virtual private network.

**ANNEX III**

# Logo Description automatically generatedStandard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

### Table 1: Parties

|  |  |  |
| --- | --- | --- |
| 1. **Start date** |  | |
| 1. **The Parties** | 1. **Exporter (who sends the Restricted Transfer)** | 1. **Importer (who receives the Restricted Transfer)** |
| 1. **Parties’ details** | 1. Full legal name: 2. Trading name (if different): 3. Main address (if a company registered address): 4. Official registration number (if any) (company number or similar identifier): | 1. Full legal name: Fundraise Up Inc. 2. Trading name (if different): 3. Main address (if a company registered address): 114 8th Street, Brooklyn, New York 11215 USA 4. Official registration number (if any) (company number or similar identifier): |
| 1. **Key Contact** | 1. Full Name (optional): 2. Job Title: 3. Contact details including email: | 1. Full Name (optional): Yuriy Smirnov 2. Job Title: Chief Technology Officer 3. Contact details including email: 718-599-1129, [legal@fundraiseup.com](mailto:legal@fundraiseup.com) |
| 1. **Signature (if required for the purposes of Section ‎2)** |  |  |

### Table 2: Selected SCCs, Modules and Selected Clauses

|  |  |
| --- | --- |
| 1. **Addendum EU SCCs** | The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:   1. Date: 2. Reference (if any): 3. Other identifier (if any): 4. Or   the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Module | 1. Module in operation | 1. Clause 7 (Docking Clause) | 1. Clause 11  (Option) | 1. Clause 9a (Prior Authorisation or General Authorisation) | 1. Clause 9a (Time period) | 1. Is personal data received from the Importer combined with personal data collected by the Exporter? |
| 1. 1 |  |  |  |  |  |  |
| 1. 2 | 1. X | 1. X | 1. X | 1. General | 1. 15f days |  |
| 1. 3 |  |  |  |  |  |  |
| 1. 4 |  |  |  |  |  |  |

### Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

|  |
| --- |
| 1. Annex 1A: List of Parties: See Annex IA of the EU SCCs. |
| 1. Annex 1B: Description of Transfer: See Annex IB of the EU SCCs. |
| 1. Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the EU SCCs. |
| 1. Annex III: List of Sub processors (Modules 2 and 3 only): General authorisation provided, list not required. |

### Table 4: Ending this Addendum when the Approved Addendum Changes

|  |  |
| --- | --- |
| 1. **Ending this Addendum when the Approved Addendum changes** | 1. Which Parties may end this Addendum as set out in Section ‎19: 2. Importer 3. Exporter 4. neither Party |

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

1. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

|  |  |
| --- | --- |
| 1. Addendum | 1. This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| 1. Addendum EU SCCs | 1. The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| 1. Appendix Information | 1. As set out in Table ‎3. |
| 1. Appropriate Safeguards | 1. The standard of protection over the personal data and of data subjects’ rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| 1. Approved Addendum | 1. The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section ‎18. |
| 1. Approved EU SCCs | 1. The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| 1. ICO | 1. The Information Commissioner. |
| 1. Restricted Transfer | 1. A transfer which is covered by Chapter V of the UK GDPR. |
| 1. UK | 1. The United Kingdom of Great Britain and Northern Ireland. |
| 1. UK Data Protection Laws | 1. All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| 1. UK GDPR | 1. As defined in section 3 of the Data Protection Act 2018. |

1. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties’ obligation to provide the Appropriate Safeguards.
2. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
3. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
4. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
5. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

### Hierarchy

1. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section ‎10 will prevail.
2. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
3. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

### Incorporation of and changes to the EU SCCs

1. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
   1. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter’s processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
   2. Sections ‎9 to ‎11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
   3. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
2. Unless the Parties have agreed alternative amendments which meet the requirements of Section ‎12, the provisions of Section ‎15 will apply.
3. No amendments to the Approved EU SCCs other than to meet the requirements of Section ‎12 may be made.
4. The following amendments to the Addendum EU SCCs (for the purpose of Section ‎12) are made:
5. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
6. In Clause 2, delete the words:

“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”;

1. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

1. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

1. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

1. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
2. References to Regulation (EU) 2018/1725 are removed;
3. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
4. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
5. Clause 13(a) and Part C of Annex I are not used;
6. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
7. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

1. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

1. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

1. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

### Amendments to this Addendum

1. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
2. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
3. From time to time, the ICO may issue a revised Approved Addendum which:
4. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
5. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

1. If the ICO issues a revised Approved Addendum under Section ‎18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
   1. its direct costs of performing its obligations under the Addendum; and/or
   2. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

1. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## Alternative Part 2 Mandatory Clauses:

|  |  |
| --- | --- |
| 1. **Mandatory Clauses** | 1. Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section ‎‎18 of those Mandatory Clauses. |