Data Processing Addendum

This Data Processing Addendum (the "**DPA**") dated below is an addendum to the Master Services Agreement executed between Benevity, Inc. ("**Benevity**") and Client (as defined in the Order Form) dated as of the Effective Date of the Order Form (the "**Agreement**"). Capitalized terms used but not defined herein shall have the meanings set forth in the Agreement.

(A) Benevity and Client entered into the Agreement that requires Benevity to process Personal Data on behalf of Client; and

(B) This DPA sets out the additional terms, requirements, and conditions on which Benevity will process Personal Data when providing services under Agreement. This DPA contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors and the General Data Protection Regulation ((EU) 2016/679).

1. *Definitions*: In this DPA, the following terms shall have the following meanings:

(a) "**Applicable Data Protection Law**" means all applicable laws and regulations relating to Processing and protection of Personal Data in force from time to time, including but not limited to the (i) European Union's General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"); (ii) in respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as saved into the United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (iii) in respect of Switzerland, the Federal Act on Data Protection ("**Swiss FADP**"); (iv) in respect of the United States, applicable federal or state information privacy laws ("**US Privacy Laws**") including but not limited to California Consumer Privacy Act, Cal. Civ. Code 1798.100 et seq., as amended including by the California Privacy Rights Act ("**CCPA**"); or (v) any other relevant applicable data protection law.

(b) "**Controller**" means a person or organization who controls the collection, holding, Processing or use of Personal Data, including a person or organization who instructs another person or organization to collect, hold, Process, use, Transfer or disclose personal information on his or her behalf.

(c) "**Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

(d) "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

(e) "**Europe**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland, and Liechtenstein ("**EEA**"), as well as, for the purposes of this DPA, Switzerland and the United Kingdom.

(f) **"International Data Transfer Agreement**" or "**IDTA**" means the template IDTA B1.0 issued by the United Kingdom's Information Commissioner's Office together with the relevant tables set out in the Annexes and Appendices of this Addendum.

(g) "**Personal Data**" means any information relating to (i) an identified or identifiable natural person, and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information) under Applicable Data Protection Law; and (iii) personal information that Benevity collects on behalf of Client or that Client shares with and/or otherwise discloses to Benevity pursuant to Agreements; and which for the purposes of the CCPA is also known as "**Covered Personal Data**".

(h) "**Processor**" means the entity which Processes Data on behalf of the Controller.

(i) "**Process**", "**Processes**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available (including the transferring of Personal Data to third-parties), alignment or combination, restriction, erasure or destruction.

(j) "**Restricted Transfer**" means: (i) where the GDPR applies, a Transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a Transfer of Personal Data from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss FADP applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

(k) "**Standard Contractual Clauses**" means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the Transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council (available as of June 2021 here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), (the "**EU SCCs**"); (ii) where UK GDPR applies, the IDTA or UK Addendum; and (iii) where the Swiss FADP applies, the EU SCCs as modified per the requirement of the Swiss Federal Data Protection and Information Commissioner ("**Swiss FDPIC**").

(l) "**Subprocessor**" means any entity which is processing Personal Data on behalf of the Processor (including any affiliate of the Processor).

(m) "**Transfer**" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to a third party or by enabling access to the Personal Data by other means.

(n) "**Transfer Impact Assessment**" means a local country assessment that evaluates the extent to which adequate protection is afforded to the Personal Data within that country, in the context of a transfer of Personal Data to the country in question, including with regards to enforcement rights and effective legal remedies of a Data Subject(s).

(o) "**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the United Kingdom's Information Commissioner's Office in accordance with the S119A(1) Data Protection Act 2018 on February 2, 2022 (as may be amended, updated or superseded from time to time by the UK Government or the Information Commissioner's Office) and attached hereto as Appendix C.

(p) For Personal Data protected by US Privacy Laws, the terms "*business*," "*business purpose*," "*commercial purpose*," "*controller*," "*processor*," "*sale*," "*sell*," "*service provider*" and "*share*" shall have the meanings given to those terms in the applicable US Privacy Laws.

1.2 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Appendices of this DPA, the provision in the body of this DPA will prevail;

(b) the terms of the Agreement and any provision contained in the Appendices of this DPA, the provision contained in the Appendices will prevail;

(c) any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail; and

(d) any of the provisions of this DPA and any executed SCC, the provisions of the executed SCC will prevail.

2. *Relationship of the Parties*: Client (the Controller) appoints Benevity as its Processor to Process the Personal Data. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law. The Client retains control of the Personal Data and remains responsible for its compliance obligations under the Applicable Data Protection Law, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Benevity.

Where applicable, with respect to US Privacy Laws, Client is a "business" or "Controller" and is engaging Benevity as a "service provider" or "Processor" to Process Covered Personal Data in the performance of the Services on behalf of Client.

Should Benevity reasonably believe that a specific Processing activity is beyond the scope of the Client's instructions but is required to comply with a legal obligation to which Benevity as Processor is subject, Benevity shall inform the Client of that legal obligation before undertaking such Processing.

3. *Purpose Limitation: Benevity shall Process the Personal Data as a Processor as* necessary to perform its obligations under the Agreement, including performing the Services specified

therein and strictly in accordance with the documented instructions of Client in a manner that does not infringe Applicable Data Protection Law (the "**Permitted Purpose**").

Without prejudice to the terms of this Clause 3, Benevity is granted a "General Written Authorisation" under Clause 9 of the Standard Contractual Clauses to transfer Personal Data to any Subprocessors named in this DPA.

In no event shall Benevity Process the Personal Data for its own purposes or those of any third party.

For Personal Data protected under applicable **US Privacy Laws (including for California residents pursuant to the California Consumer Privacy Act ("CCPA"))**, any Processing of Covered Personal Data, is not for monetary or other valuable consideration, but instead to support the Services pursuant to the Agreement, and therefore does not constitute a sale of Covered Personal Data to Benevity. The Processor is expressly prohibited from selling or sharing the Covered Personal Data, retaining, using or disclosing the Covered Personal Data for any other purpose other than the specific purpose of performing the Services including retaining, using, or disclosing the Covered Personal Data for a commercial purpose other than providing the Services; and retaining, using, or disclosing the information outside of the direct business relationship.

4. *International Transfers:* Benevity shall not Transfer the Personal Data (nor permit the Personal Data to be Transferred) across country borders unless: (a) it has first obtained Client's prior written consent; (b) it takes measures as are necessary and legally required, such as entering into applicable Standard Contractual Clauses, to ensure the Transfer is in compliance with Applicable Data Protection Law; and (c) it has implemented all necessary additional measures and safeguards as required by Applicable Data Protection Laws. Client hereby consents to the Transfer of Personal Data between Canada and the United States and across country borders as may be required to facilitate the Services, further, and for the avoidance of doubt (and where applicable only), the Client hereby consents to the appointment by Benevity of Subprocessors located outside the UK and the EEA, and the Client authorizes Benvity to enter into the SCCs contained in this DPA with such of its Subprocessors as is appropriate.

5. *Confidentiality of Processing:* Benevity shall ensure that any person that it authorizes to Process the Personal Data (including Benevity's staff, agents and subcontractors) (an "**Authorized Person(s)**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to Process the Personal Data who is not under such a duty of confidentiality. Benevity shall ensure that all Authorized Persons process the Personal Data only as necessary for the Permitted Purpose.

6. *Security:* Benevity shall implement appropriate technical and organizational measures to protect the Personal Data from Data Breaches in accordance with Benevity's Information Security Addendum available here (https://benevity.com/information-security-addendum). Such measures shall have regard to 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. At a minimum, such measures shall include the measures identified in Annex II to the Standard Contractual Clauses, listed at Appendix B of this DPA.

Additionally, Benevity will ensure that, as appropriate, its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Applicable Data Protection Law relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware of their duties and obligations to support the Security measures set out in Annex II to the Standard Contractual Clauses in Appendix B of this DPA.

7. *Subprocessing:* Client hereby confirms the General Written Authorization as at the date of this DPA for the use of the list of Subprocessors attached at Appendix A. Where Benevity engages a new Subprocessor to Process Personal Data, Benevity shall provide written notification to Client with at least thirty (30) days' prior notice before the addition of any new Subprocessor, including details of the scope of Processing it performs or will perform and the location and identity of the Subprocessor. For each new Subprocessor, Benevity shall: (a) conduct adequate due diligence on the Subprocessor to ensure it is capable of providing the level of protection of Personal Data required by this DPA; (b) impose data protection terms on Subprocessor that protect the Personal Data to the same standard provided for by this DPA; and (d) Benevity remains fully liable for any breach of this DPA that is caused by an act, error or omission of its Subprocessor. In the event that Client objects to the processing of its Personal Data by any proposed Sub-processor on reasonable grounds relating to data protection, Client shall inform Benevity in writing by emailing privacy@benevity.com within thirty (30) days of initial notification. In such an event, the Parties shall negotiate in good faith a solution to Client’s objection. If the Parties cannot reach resolution within thirty (30) days of Benevity’s receipt of Client’s objection, Benevity will either (a) instruct the Subprocessor not to process Client's Personal Data, in which event this DPA shall continue unaffected, or (b) Client may elect to suspend or terminate the Agreement without penalty.

If Client terminates the Agreement pursuant to this Section 7, it does so without penalty or liability (other than for fees due and owing to Benevity for services performed prior to such termination).

8. *Cooperation and Data Subjects’ Rights:* Taking into account the nature of the Processing, Benevity shall provide assistance (including by appropriate technical and organizational measures) to Client to enable Client to respond to: (a) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Personal Data (together, a “Request”). In the event that any such Request is made directly to Benevity, Benevity shall promptly inform the Client providing full details of the same.

9. *Regulator Requests:* Benevity will promptly notify Client of any complaints or any notices of investigation or non-compliance received from any Regulator related to the collection or Processing of Data ("Regulator Requests"). Unless Benevity is responsible for handling a particular communication or correspondence with a Regulator under Applicable Data Protection Law, in which case it will notify Client of the same promptly and prior to sending out any communication, unless required to do otherwise by Applicable Data Protection Law, Client will handle all communications and correspondence with Regulators relating to Data and the provision or receipt of the Services.

   Benevity will make all reasonable efforts to cooperate with Client and the relevant Regulator in the event of any investigation or litigation concerning Data and shall abide by the direction or request of the relevant Regulator with regard to the Processing of such Data.

   Benevity will not make transfers of Data to any law enforcement or security authorities or other government agencies in breach of relevant Applicable Data Protection Law or the Agreement, unless such transfer is required under applicable law.

10. *Data Protection Impact Assessment:* Taking into account the nature, scope, context and purposes of the Processing, if the Client directs, or if Benevity believes or becomes aware that its Processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Client and provide Client with all such reasonable and timely assistance as Client may require in order to conduct a Transfer Impact Assessment.

11. *Data Breaches:* Upon becoming aware of a Data Breach affecting the Client's Personal Data, Benevity shall inform Client without undue delay. Benevity shall provide all such timely information and cooperation as Client may require in order for Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Such notification shall include, at a minimum: (a) a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned); (b) details of a contact point where more information can be obtained; (c) a description of the likely consequences of the Data Breach; and (d) a description of the measures taken or proposed to address the Data Breach, including measures to mitigate its possible adverse effects. Benevity shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Personal Data Breach and shall keep Client up-to-date about all developments in connection with the Personal Data Breach.

12. *Deletion or Return of Personal Data:* Upon termination or expiry of the Agreement, Benevity shall (at Client's election) destroy or return to Client all Personal Data (including all copies of the Personal Data) in its possession or control (including any Personal Data subcontracted to a third party for Processing). Notwithstanding the foregoing, and only to the extent necessary for the prevention of fraud and to adhere to taxation record retention requirements, Benevity retains Personal Data pertaining to donation transactions in accordance with requirements under applicable laws, but in general for seven (7) years from the date of termination of the Agreement. The requirement to

destroy or return herein shall also not apply to the extent that Benevity is required by any other applicable law to retain some or all of the Personal Data. In the event of any of the foregoing exceptions, Benevity shall isolate and protect the Personal Data from any further Processing except to the extent required for fraud prevention or by such law. In all cases, for so long as Personal Data is retained in accordance with this Section 11: (i) the obligations of confidentiality and security set out in the Agreement and this DPA shall apply in relation to that Personal Data; (ii) the Personal Data will not be used for any commercial purpose; and (iii) the Personal Data will be deleted or otherwise destroyed in a timely manner in accordance with Benevity's document management/destruction policies.

13. *Security Package, Audit and Inspection:*

(a) **Security Package**. Benevity will make available to Client, without charge, Benevity's Trust & Security self-serve portal (available on B-Hive) which includes: (i) Benevity's audit reports performed by an independent third-party auditor; (ii) Benevity's hosting provider's audit report; (iii) PCI DSS attestations of compliance from payment processors used; (iv) information on Benevity's information security and privacy programs; and (v) a completed industry-standard information security questionnaires and frequently asked questions (together the "**Security Package**''), to assist with Client's risk assessment & compliance requirements. Benevity will assist Clients with reasonable inquiries or clarifications, and items that may not be covered by the Security Package. Please find B-Hive Trust & Security self-serve portal below:
https://b-hive.benevity.com/hc/en-us/categories/4411210830356-Trust-and-Security

Where a Client requests to complete custom security questionnaires, or where responses are duplicative of material available in the Security Package, Benevity may charge a reasonable agreed-upon fee to the Client for such additional assistance.

(b) **Audit and Inspection**. To the extent the Client's audit obligations under Applicable Data Protection Laws are not reasonably satisfied through the Essentials Security Package, Benevity shall permit Client (or its third-party auditors) to inspect or audit for Benevity's compliance with this DPA to the extent required by Applicable Data Protection Law with mutual agreement on scope, timing and duration, provided that Client gives at least thirty (30) days' prior notice of its intention to inspect or audit, conducts its inspection or audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Benevity's operations. Client shall ensure that its personnel (or its third-party auditors) adhere to Benevity's reasonable internal security measures and are bound to confidentiality obligations no less stringent than those in the Agreement. Except for an audit or inspection as a result of Section 13 (c) (i) and (ii) below, Benevity will charge a reasonable agreed-upon fee to Client for such additional assistance.

(c) **Annual Request**. Client will not exercise its audit and inspection rights more than once in any twelve (12) calendar month period, except: (i) if and when required by instruction of a competent data protection authority, Applicable Data Protection Law or the Standard Contractual Clauses; (ii) Client is seeking information at the request of a competent data protection authority which cannot otherwise be reasonably obtained from Benevity or through the use of the Essentials Security Package; or (iii) Client reasonably believes a further audit is necessary due to a Data Breach suffered by Benevity.

14. *Limitation of Liability* This DPA shall be subject to the limitations of liability agreed between the Parties set forth in the Agreement and any reference to the liability of a Party means that Party and its Affiliates in the aggregate. For the avoidance of doubt, Client acknowledges and agrees that Benevity's total liability for all claims from Client or its Affiliate arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA.

    This section shall not be construed as limiting the liability of either Party with respect to claims brought by data subjects or under the EU SCCs' Clause 12 and/or and/or the UK Addendum.

15. *Standard Contractual Clauses:* The parties agree that when the Transfer of Personal Data from Client (as "data exporter") to Benevity (as "data importer") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the Parties will be subject to the relevant Standard Contractual Clause(s) attached to this DPA as modified by the attached appendices for transfers of Personal Data from the United Kingdom and Switzerland. The relevant Standard Contractual Clause(s) are set out in full below, but for reference, they will incorporated into and form part of this DPA as follows:

    (a) In relation to Transfers of Personal Data protected by the GDPR, the EU SCCs will be completed as follows:

    (i) the clauses as set forth in Module Two (Controller to Processor) shall apply;

    (ii) the "data exporter" is the Client and the data exporter's contact information is set forth in Appendix B;

    (iii) the "data importer" is Benevity, and Benevity's contact information is set forth in Appendix B;

    (iv) in Clause 7, the optional docking clause will apply;

    (v) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes will be as set out in Section 7 of this DPA;

    (vi) in Clause 11, the optional language will not apply;

    (vii) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

    (viii) in Clause 18(b), disputes will be resolved before the courts of Ireland; and

    (b) In the event that the SCCs are at any time no longer deemed to provide adequate protection to Personal Data transferred to Third Country Recipients, the parties shall enter into and/or adopt such alternative data transfer solution to replace the SCCs as is required by the European Commission or the appropriate Regulator to comply with Applicable Data Protection Law.

16. Subject to terms required by Applicable Data Protection Law, the term of this DPA shall be for the period in which the Agreement remains in force ("**DPA Term**") and shall not be terminated prior to the end of the DPA Term unless there is a material breach of this DPA or the parties agree in writing.

Accepted and agreed to by the authorized representatives of each party:

[CLIENT]

By: ______________________________

Name: __________________________

Title: ____________________________

Date: ____________________________

Benevity, Inc.

By: ____________________________

Name: __________________________

Title: ___________________________

Date: __________________________

Appendix A - Approved Subprocessors

(for the purposes of the UK Addendum, this Appendix is to be labelled as Annex III, under Part 1, Table 3)

Benevity maintains a current list of current Subprocessors at: https://benevity.com/subprocessors.

Name	Description of Processing	Location	Transfer Mechanism
Amazon Web Services, Inc.	Data centre and cloud infrastructure as a service provider. Benevity manages encryption keys. AWS has no access to client data within Benevity infrastructure	US	EU SCCs / UK Addendum
Atlassian Pty Ltd	Source code repository and ticketing system for production issues and changes. Atlassian has no access to data within Benevity's instance.	US	EU SCCs / UK Addendum
BlueSnap, Inc.	Credit card payment processing for donors. May receive donor name, address and email only. Benevity does not collect, store or process any sensitive cardholder data (PAN, expiry, CVC)	US, UK (Recovery Site)	EU SCCs / UK Addendum for US. Adequacy decision for UK
Boomi, Inc.	Platform integration cloud provider to manage Workday integration for payroll deductions. Benevity manages encryption keys. Boomi has no access to client data with Benevity infrastructure	US	EU SCCs / UK Addendum
Google, Inc.	Data warehouse, corporate document storage and cloud infrastructure as a service provider. Benevity manages encryption keys. Google has no access to client data within Benevity infrastructure	US	EU SCCs / UK Addendum
ModSquad, Inc.	Subcontractor services to supplement Benevity Technical Support teams.	US	EU SCCs / UK Addendum
The Rocket Science Group LLC dba Mailchimp	Email template and delivery to users	US	EU SCCs / UK Addendum
Okta, Inc.	Identity and authentication management for Benevity systems and applications. Benevity manages encryption keys. OKTA has no access to client data within Benevity instance	US	EU SCCs / UK Addendum
OpenAI, LLC	Generative artificial intelligence support for Benevity systems and processes. Benevity does not use client data to build or train models.	US	EU SCCs / UK Addendum
PayPal, Inc.	Credit card payment processing for donors. May receive name, address and email only.	US	EU SCCs / UK Addendum

Name	Description of Processing	Location	Transfer Mechanism
	Benevity does not collect, store or process any sensitive cardholder data (PAN, Expiry, CVC)		
Pendo.io, Inc	Product Analytics and User Feedback	EU	EU SCCs / UK Addendum
Ping Identity Corporation	Single Sign On provider for integration with clients identity provider (IPD).	US	EU SCCs / UK Addendum
strongDM, Inc.	Access management and event logging for database infrastructure for Benevity teams. StrongDM has no access to client data.	US	EU SCCs / UK Addendum
Ninja Partners LLC dba SupportNinja	Subcontractor services to supplement Benevity End User Care teams	US and Philippines	EU SCCs / UK Addendum
Surecall Contact Centers Ltd.	Subcontractor services to supplement Benevity End User Care teams	Canada and US	EU SCCs / UK Addendum. Adequacy decision for Canada
trycourier.com, Inc.	User notification preferences management software	US	EU SCCs / UK Addendum
Zendesk, Inc	Client ticketing and user support platform	US	EU SCCs / UK Addendum

Appendix B

EU Standard Contractual Clauses (Module Two: Transfer 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 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.

(d) 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 8.1(b), 8.9(a), (c), (d) and (e);
- (iii) Clause 9(a), (c), (d) and (e);
- (iv) Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18(a) and (b).

(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 – Optional

Docking clause

(a) 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.

(b) 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.

(c) 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

(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 benefiting 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) OPTION 2: 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 thirty (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 1

(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.

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

Clause 17

Governing law

OPTION 2: 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 Ireland.

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 Ireland.

(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 I to the EU Standard Contractual Clauses

Data Processing Activities

MODULE TWO: Transfer controller to processor

A. List of Parties

Data Exporter

Name:	Client, a user of the Services in the Agreement
Address:	Address as listed in the Agreement
Contact person's name, position and contact details:	Contact information as listed in the Agreement
Activities relevant to the data transferred under these Clauses:	The data exporter has licensed certain software and associated technology of the data importer and utilizes data importer's support services to enable and facilitate the administration of aspects of the data exporter's corporate social responsibility and charitable giving programs. The data exporter will transfer personal data of authorized users (e.g. the data exporter's employees) to the data importer, which will be hosted by a third-party data hosting facility, currently located in the United States. The data exporter consents to the transfer of personal data to the data importer's third-party hosting facility
Signature:	
Date:	
Role (controller/processor):	Controller

Data Importer

Name:	Benevity, Inc., provider of the Services
Address:	#700, 611 Meredith Road NE, Calgary, Alberta, T2E 2W5
Contact person's name, position and contact details:	Director, Risk & Compliance, privacy@benevity.com
Activities relevant to the data transferred under these Clauses:	The software, associated technology and support services licensed or utilized by the data exporter requires personal data such as name and business e-mail address for identity verification and sign-on. In some cases, home address and other personal data of the data subject is provided by the data subject to access certain functionality, such as the generation of charitable tax receipts.
Signature:	
Date:	
Role (controller/processor):	Processor

B. Description of Transfer

Categories of data subjects whose personal data is transferred

Users authorized by the data exporter to use the software. This may include employees, contractors or any other person authorized by the data exporter to be provided with access to the software.

- Clients' workforce, including employees, contractors, volunteers, temporary and casual workers, and other personnel or workforce members

Categories of personal data transferred

The personal data transferred pursuant to these Clauses is determined by the data exporter in its sole discretion, and may include, without limitation, the following categories of data:

- Basic Contact information: First and last name, email address
- Business contact information, such as company name, business email, phone, business address, business unit, office or division, geographic business location, job title or role, reporting lines;
- Employment information, such as employee, payroll or workforce ID number;
- Transactional information such as giving, volunteering, Personal data pertaining to donation transactions (as defined below).
- Technical information related to data subjects, their systems or devices, and/or the use of their or third party systems or devices, including IP addresses, location data, usage data, usernames and other account information or credentials.
- Categories of personal data as otherwise agreed upon between Client and Service Provider in Agreements, including its exhibits, appendices, attachments and amendments.

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 is transferred.

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

Continuous with use of the Services as described in the Agreement.

Nature of the processing

The provision of the Services to Client in accordance with the Agreement.

Purpose(s) of the data transfer and further processing

Benevity will process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Client in the use of the Services. To enable and facilitate the administration of aspects of the data exporter's corporate social responsibility and charitable giving programs.

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

Personal data pertaining to donation transactions made through the platform must be retained in accordance with applicable income tax laws, generally around 7 years, depending on the tax jurisdiction.

Specifically, Personal data pertaining to donation transactions is what is required to prepare a tax-deductible receipt, acceptable in accordance with applicable income tax law. This includes:

- Donors first and last name
- Donor’s business email
- Donor’s address for tax deductible receipt
- Date of donation
- Nominated cause
- Donation amount
- Donor’s comments shared with cause, if any

All other Personal data will only be retained as per client instructions for the duration of the contract. Personal data may be deleted (anonymized) upon request of the data subject, or per Client instructions.

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

The subject matter, nature and duration of the processing are specified above and in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

Client agrees the competent supervisory authority will be the Data Protection Commission (DPC) of Ireland.

Annex II to the EU Standard Contractual Clauses

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

MODULE TWO: Transfer controller to processor
Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The data importer has implemented an information security management system (ISMS) based on industry leading standards ISO 27001 and COBIT. This system is governed by a dedicated Risk & Compliance function, which oversees related policies, procedures, and controls related to technical and organizational security measures related to safeguarding client information.

A description of Benevity's current technical and organizational security measures can be found in Benevity's Information Security Addendum "ISA". Benevity reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this document.
https://benevity.com/information-security-addendum.

Specific measures*:*

Measure	***Description***
Measures of pseudonymisation and encryption of personal data	Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to Benevity is encrypted with 256-bit encryption and supports TLS 1.2 and above.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Benevity maintains an information security program, which includes: (a) having a formal risk management program; (b) conducting periodic risk assessments of all systems and networks that process Data on at least an annual basis; (c) monitoring for security incidents and maintaining a tiered remediation plan to ensure timely fixes to any discovered vulnerabilities; (d) a written information security policy and incident response plan that explicitly addresses and provides guidance to its personnel in furtherance of the security, confidentiality, integrity, and availability of Data; (e) penetration testing performed by a qualified third party on an annual basis; and (f) having resources responsible for information security efforts.
Measures for ensuring the ability to restore the availability	Benevity takes daily snapshots of its databases and securely copies them to a separate data centre for

Measure	***Description***
and access to personal data in a timely manner in the event of a physical or technical incident	recovery purposes in the event of a regional AWS failure. Backups are encrypted and have the same protection in place as production. Additionally, Data is stored cross-regionally with AWS.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	On an annual basis, Benevity performs on its own and engages third parties to perform a variety of testing to protect against unauthorized access to Data and to assess the security, reliability, and integrity of the Services. To the extent Benevity determines, in its sole discretion, that any remediation is required based on the results of such testing, it will perform such remediation within a reasonable period of time taking into account the nature and severity of the identified issue. As of the Effective Date, Benevity undergoes annual independent external audits with respect to processing of its information security programme and systems.
Measures for user identification and authorisation	Access to manage Benevity's AWS environment requires multi-factor authentication, access to the Services is logged, and access to Data is restricted to a limited set of approved Benevity employees. AWS networking features such as security groups are leveraged to restrict access to AWS instances and resources and are configured to restrict access using the principle of least privilege. Employees are trained on documented information security and privacy procedures. Every Benevity employee signs a confidentiality agreement that binds them to the terms of Benevity's data confidentiality policies and access to Benevity systems is promptly revoked upon termination of employment.
Measures for the protection of data during transmission	Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to Benevity is encrypted with 256-bit encryption and supports TLS 1.2 and above.
Measures for the protection of data during storage	Data is stored cross-regionally with AWS. Data backups are encrypted. Data is encrypted at rest with AES 256-bit secret keys.

Measure	***Description***
Measures for ensuring physical security of locations at which personal data are processed	Benevity uses Amazon Web Services (AWS) (and such cloud hosting providers as may be appropriate to employ from time to time) to provide management and hosting of production servers and databases in the United States. AWS employs a robust physical security program with multiple certifications, including SOC 2 and ISO 27001.
Measures for ensuring events logging	All access to information security management systems at Benevity are restricted, monitored, and logged. At a minimum, log entries include date, timestamp, action performed, and the user ID or device ID of the action performed. The level of additional detail to be recorded by each audit log will be proportional to the amount and sensitivity of the information stored and/or processed on that system. Read-only copies of all system logs are streamed in real-time to Benevity’s read-only log server to prevent tampering.
Measures for ensuring system configuration, including default configuration	Benevity leverages centrally managed images to generate virtual systems in Benevity’s AWS environment. We leverage “Infrastructure as Code” scripts to automate numerous security configurations that align to industry best practices, where each configuration undergoes integrity monitoring to detect and alert for any deviations to industry standards.
Measures for internal IT and IT security governance and management	Benevity maintains a formal information security program with dedicated security personnel reporting to Benevity’s Security Operations Manager. Benevity’s Security Operations Team is responsible for implementing security controls and monitoring Benevity for suspicious activity. Policies and procedures, including the Benevity IT Security Policy, are updated on an annual basis and reviewed and approved by Management. Benevity's Risk & Compliance team has developed a formal risk management approach to be used for all risk assessments and evaluations. The approach is based on the ISO 31000 framework and defines the process for risk identification, analysis, ownership, evaluation and treatment.

Measure	***Description***
Measures for certification/assurance of processes and products	As of the Effective Date, Benevity undergoes annual independent external audits with respect to processing of its information security programme and systems.
Measures for ensuring data minimisation	Benevity only collects information that is necessary in order to provide the Services outlined in the Agreement. Benevity's employees are directed to access only the minimum amount of information necessary to perform the task at hand.
Measures for ensuring data quality	Benevity maintains logs for user activity and security events at the network, operating system, database, and application levels. Read-only copies of all system logs are streamed in real-time to Benevity's read-only log server to prevent tampering. At minimum, log entries include date, timestamp, action performed, and the user ID or the device ID of the action performed. Users who would like to exercise their rights under Applicable Data Protection Law to update information which is out of date or incorrect may do so at any time by contacting Benevity at privacy@benevity.com. More information on Data Subject rights can be found at https://benevity.com/privacy-policy.
Measures for ensuring limited data retention	Benevity will retain information for the period necessary to fulfil the purposes outlined in Benevity's Privacy Policy at https://www.benevity.com/privacy-policy, or where the Agreement requires or permits specific retention or deletion periods. Users who would like to exercise their rights under Applicable Data Protection Law to update information which is out of date or incorrect may do so at any time by contacting Benevity at privacy@benevity.com. More information on Data Subject rights can be found at https://benevity.com/privacy-policy.
Measures for ensuring accountability	Benevity has established a comprehensive GDPR privacy compliance program and is committed to partnering with its clients and vendors on GDPR compliance efforts. Some significant steps Benevity has taken to align its practices with the GDPR include: • Enhancements to Benevity's security practices and procedures

Measure	***Description***
	• Closely reviewing and mapping the data Benevity collects, uses, and shares • Creating more robust internal privacy and security documentation • Training employees on GDPR and Privacy requirements and privacy and security best practices generally • Appointed a Data Protection Officer ("DPO"), who can be reached at privacy@benevity.com. Users who would like to exercise their rights under Applicable Data Protection Law to update information which is out of date or incorrect may do so at any time by contacting Benevity at privacy@benevity.com. More information on Data Subject rights can be found at https://benevity.com/privacy-policy.
Measures for allowing data portability and ensuring erasure	Benevity provides a mechanism for individuals to exercise their privacy rights in accordance with Applicable Data Protection Law. Individuals may contact exercise their rights by contacting Benevity at privacy@benevity.com

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

As described in this DPA, Benevity has measures in place to provide assistance to controllers as needed. Such measures include, but are not limited to, the ability to delete all Data associated with the Services, subject to Applicable Data Protection Law. With regard to Data Subject Requests, in the event the controller is unable to address a Data Subject Request in its use of the Service, Benevity will, upon request, provide commercially reasonable efforts to assist the controller in responding to such Data Subject Request, to the extent Benevity is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Law. Data Subjects may also exercise their rights by contacting Benevity at privacy@benevity.com.

APPENDIX C – UK ADDENDUM

To the extent applicable, this **UK Addendum Exhibit** is incorporated into the DPA. If there is any conflict between any provision of the UK Addendum and any provision of the DPA or any other agreement (including without limitation any other exhibit, schedule, or other attachment thereto), then the provision of the UK Addendum will control to the extent of such conflict with respect to the Personal Data that is subject to the UK Addendum.

In the event of a Restricted Transfer, the parties enter into this Addendum as issued by the ICO and as amended from time to time to the extent necessary to operate to provide Appropriate Safeguards for Restricted Transfers in accordance with Article 46 of the UK GDPR.

PART 1: TABLES	
TABLE 1	
PARTIES	The Parties are set out in Annex I.A. of the Appendix to the Approved EU SCCs.
TABLE 2	
SELECTED SCCS, MODULES AND SELECTED CLAUSES	The version of the Approved EU SCCs is attached at Appendix B to the DPA.
TABLE 3	
APPENDIX INFORMATION	Annex I.A: List of Parties: See the details for the data exporters and data importer(s) provided at Annex I.A. to the Appendix of the version of the Approved EU SCCs.
	Annex I.B: Description of Transfer: See the description of transfer provided at Annex I.B. of the Appendix to the Approved EU SCCs.
	Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the Appendix to the Approved EU SCCs.
	Annex III: List of Sub processors: See the details relating to sub-processors provided at Annex I.B. of the Appendix to the Approved EU SCCs and in Appendix A of the DPA.
TABLE 4	
ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES	Neither Party shall have the right to end this Addendum pursuant to Section 19.

PART 2: MANDATORY CLAUSES
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

APPENDIX D – SWITZERLAND ADDENDUM TO THE SCCs

Where the Standard Contractual Clauses apply to a transfer of Personal Data to which the Swiss FADP applies, the Standard Contractual Clauses shall be deemed to be amended to the extent necessary to operate to provide appropriate safeguards for such transfers in accordance with the Swiss FADP, including without limitation the following:

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

(ii) the term "Member State" cannot be interpreted to exclude data subjects in Switzerland from exercising their rights under Data Protection Law;

(iii) the term "personal data" shall be deemed to include the data of legal entities to the extent such data is protected under the Swiss FADP; and

(iv) any amendments required from time to time by the Federal Data Protection and Information Commissioner in order to comply with the Swiss FADP.

[END OF DPA]