Appendix A

Approved Subprocessors

(if applicable, Part 1, Table 3, Annex III to the UK Addendum)

Name	Description of Processing	Location	Transfer Mechanism
Amazon Web Services, Inc.	Data center 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	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
Box.com (UK) Ltd	Corporate document storage provider. Benevity manages encryption keys. Box has no access to client data within Benevity infrastructure	US	EU SCCs / UK Addendum
Google, Inc.	Data warehouse 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
Onspring Technologies, LLC	GRC solutions to track and manage incidents and investigations	US	EU SCCs / UK Addendum
PayPal, Inc.	Credit card payment processing for donors. May receive name, address and email only. Benevity does not collect, store or process any sensitive cardholder data (PAN, Expiry, CVC)	US	EU SCCs / UK Addendum
Ping Identity Corporation	Single Sign On provider for integration with clients identify 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
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 – Data Processing Activities

(Annex I to the EU Standard Contractual Clauses and, as applicable, Part 1, Table 3, Annex 1A and 1B to the UK Addendum)

A. List of Parties

MODULE TWO: Transfer controller to processor

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 Amazon Web Services Inc., which is located in the United States. The data exporter consents to the transfer of personal data to the data importer's third-party hosting facility, Amazon Web Services Inc. (AWS). The AWS GDPR Data Processing Addendum which includes EU Standard Contractual Clauses between the data importer and the subprocessor is located at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
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***

MODULE TWO: Transfer controller to processor

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.

Categories of personal data transferred

Business contact information (name and business e-mail address) in all cases. Additional personal data by the data subject directly (address) to access specific software functionality.

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

To enable and facilitate the administration of aspects of the data exporter’s corporate social responsibility and charitable giving programs.

Except as limited by applicable law or the other agreements between data importer and data exporter, data importer's System and Services may be used to process Personal Data for purposes of conducting testing (for example, to ensure that Personal Data intended to be used in the System or by the Services is used accurately), development (for example, to determine more efficient ways to process Personal Data within data importer's System or Services), and training (for example, to train internal users of data exporters how to use Personal Data within data importer's System or with data importer's Services).

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

Seven years after the termination of the Agreement.

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.

Appendix C – Security Measures

(if applicable, Annex II to the EU Standard Contractual Clauses and Part 1, Table 3 Annex II of the UK Addendum)

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 at: https://benevity.com/security

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 and access to personal data in a timely manner in the event of a physical or technical incident	Benevity takes daily snapshots of its databases and securely copies them to a separate data center for 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	On an annual basis, Benevity performs on its own

testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	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.
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.
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 • 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 D – 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. Any personal data described in the UK Addendum is included in the definition of Personal Data. Part 1: Table 2 should be interpreted as referencing the EU Standard Contractual Clauses (module Controller to Processor) as completed in the EU Standard Contractual Clauses Exhibit.

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

3. 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:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	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.
Approved Addendum	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.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	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.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. 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.
5. 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.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. 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.
8. 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

9. 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.
10. 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.
11. 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

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. 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;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. 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.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
    b. 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";

    c. 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.";

    d. 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";

    e. 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;"

    f. 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;
    g. References to Regulation (EU) 2018/1725 are removed;
    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
    j. Clause 13(a) and Part C of Annex I are not used;
    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
    l. 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;";

    m. Clause 17 is replaced with:
        "These Clauses are governed by the laws of England and Wales.";

    n. 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

o. 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

16. 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.
17. 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.
18. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. 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.
19. 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:
    a its direct costs of performing its obligations under the Addendum; and/or
    b 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.
20. 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.

[END OF DPA]