

Data Processing Addendum (DPA)

Version 2, March 10, 2026

This Data Processing Addendum ("DPA") forms a part of and is subject to The Giving Step's Master Subscription Agreement, applicable Order Form or Statement of Work or other written subscription agreement (together with any attachments issued thereunder, the "Agreement") between The Giving Step, LLC ("Company", "TGS") and the Party identified as the "Customer" in the Agreement, where Customer is using Company's Software and Services. This DPA reflects the Parties' agreement with regards to the applicable Privacy/Data Protection Laws and governs the data processing related obligations of Company and Customer for any applicable Order Form or Statement of Work involving the processing of Customer's Personal Information. In the event of any inconsistency or conflict between this DPA and the Agreement, the terms and conditions of the DPA shall prevail.

In delivering the Software or Services under the Agreement, Company may Process Personal Information/ Personal Data as a Data Processor on behalf of Customer, which is the data controller. It is hereby agreed as follows:

1. Definitions.

1.1. All capitalized terms not specifically defined in this DPA shall have the same meaning as provided for in the Agreement. Terms used but not defined in the Agreement or in this Section 1 (Definitions), will have the same meaning as set forth in Article 4 of the GDPR.

1.2. "Contracted Processor" means Company or a Sub-Processor.

1.3. "Data Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of the Personal Information/ Personal Data, or as otherwise specified in applicable Privacy/Data Protection Laws.

1.4. "Data Processor" means a natural or legal person, public authority or other body which processes Personal Information/ Personal Data on behalf of the Data Controller, or as otherwise specified in applicable Privacy/Data Protection Laws.

1.5. "Data Subject" means an identified or identifiable natural person. "Data Subject" shall be understood to include "Consumer" and analogous terms under Privacy Laws.

1.6. "Incident" means a situation whereby Personal Data in either Processor's or any Authorized Person's systems, backups, networks, servers, databases, computers, or other hardware or technical infrastructure, was lost or is reasonably likely to be lost with a risk of potential harm or damage to Data Subjects.

1.7. "Industry Standards" means the then-current industry best data protection and data processing practices relating to the Processing of the Personal Data.

1.8. "Personal Data Breach" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Data.

1.9. "Personal Information/ Personal Data" means any information relating to an identified or identifiable natural person that is stored, Processed, or transmitted in connection with, or as a result of, providing the Software or Services or as may otherwise be specified in applicable Privacy/Data Protection Laws. Personal Information/Personal Data shall include any information that is Processed in connection with the Services (i) relating to an identified or identifiable natural person, or (ii) that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household (including, without limitation, the data elements listed in section 1798.140(o)(1)(A)-(K) of the CCPA and CPRA if any such data element identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household).

1.10. "Privacy/Data Protection Laws" means any and/or all domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to data privacy, data security and/or the protection of Personal Information/ Personal Data, including but not limited to the Regulation EU 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of Personal Information / Personal Data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulations" or "GDPR") and the laws implementing or supplementing the GDPR, including each EU Member States' national implementation thereof; (ii) the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the Swiss Federal Act on Data Protection ("Swiss FADP"); (iv) the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., ("CCPA") as amended by the California

Privacy Rights Act ("CPRA"); (v) Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act) ("CPA"); (vi) Connecticut's Data Privacy Act ("CTDPA"); (vii) Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act) ("UCPA"); and (viii) VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("VCDPA"); (ix) the Canadian Personal Information Protection and Electronic Documents Act, SC 2000, c 5 ("PIPEDA"), and any successor legislation or regulations thereto.

1.11. "Process," "Processing," or "Processed" means an operation or set of operations that is performed upon Personal Information/ Personal Data, whether or not by automatic means, including, collection, recording, organization, storage, access, transmission, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, disposal, deleting, erasure, or destruction.

1.12. "Restricted Transfer" means:

1.12.1. a transfer of Customer Personal Data from Customer to a Contracted Processor; or

1.12.2. an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor, in each case:

1.12.3. where the EU GDPR applies, such transfer of Customer Personal Data is to a country outside of the European Economic Area which is not subject to an adequacy determination by the Commission; and

1.12.4. where the UK GDPR applies, such transfer of Customer Personal Data is to a country outside of the United Kingdom which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

1.12.5. where the Swiss FADP applies, such transfer of Customer Personal Data is to a country outside of Switzerland which is not subject to an adequacy determination by the Swiss Federal Data Protection and Information Commission; or

1.12.6. where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established below;

1.13. "Secondary Customer" means a customer which has entered into a Data Processing Agreement with Customer or a Customer Affiliate.

1.14. "Security Incident" means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to Personal Information/ Personal Data or an incident that presents a risk to the security of the network and information systems.

1.15. "Standard Contractual Clauses" means: (i) where the EU GDPR applies or where the Swiss FADP applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 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 the Council ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

1.16. "Sub-processor" means any third party (including any Processor's Affiliate) engaged by Processor to Process any Personal Information/ Personal Data relating to this DPA and/or the Contracts.

1.17 "Technical and Organizational Security Measures" means measures taken by Processor and Authorized Persons aimed at (i) ensuring the confidentiality, security, integrity, and availability of Personal Data, including protecting against an Incident, a Personal Data Breach, or other accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access to Personal Data (in particular where Processing involves the transmission of Personal Data over a network) and other unlawful forms of Processing and/or (ii) assisting and enabling Data Controller to comply with its obligations to respond to requests by Data Subjects to exercise their Data Subject Rights.

2. Subject and Scope.

2.1. To the extent Processing of Personal Information/ Personal Data takes place with respect to Data Subjects in the United Kingdom, the UK GDPR and this DPA will apply. To the extent Processing of Personal Information / Personal Data takes place with respect to Data Subjects in the European Union, the GDPR and this DPA will apply. To the extent Processing of Personal Information/Personal Data takes place with respect to Data Subjects in Switzerland, the Swiss FADP and this DPA will apply. To the extent Processing of Personal Information/ Personal Data pertains to a California resident the CCPA, CPRA and this DPA shall apply. To the extent Processing of Personal Information / Personal data pertains to a resident in another US state with an applicable Privacy/Data Protection Law, such law and this DPA shall apply.

2.2. Company shall Process Personal Information/ Personal Data under the Agreement(s) only as a processor acting on behalf of Customer where Customer is the Data Controller, as a Sub-Data Processor acting on behalf of Customer where Customer is a Data Processor or as Sub-Sub-Data Processor where Customer is a Sub-Data Processor. Company agrees that it will Process Personal Information/ Personal Data for the sole purpose of providing the Services as described in the Agreement(s).

2.3. Customer discloses Personal Information/ Personal Data to Company solely for: (i) a valid business purpose; and (ii) Company to perform the Services.

2.4. Subject to the CCPA and CPRA, Company is prohibited from: (i) selling or sharing Personal Information/ Personal Data; (ii) retaining, using, or disclosing Personal Information/ Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Information/ Personal Data outside of the Agreement between Company and Customer.

2.5. As necessary for the provision of the Software and Services, Customer instructs Company (and authorizes Company to instruct each Sub-processor) to:

2.5.1. Process Personal Information/ Personal Data, including but not limited to by disclosing such data to Sub-processors and Affiliates;

2.5.2. transfer Personal Information/ Personal Data to any country or territory subject to Section 5; and

2.5.3. engage any Sub-processors subject to Section 4.

2.6. Customer warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give such instruction.

2.7. Customer is solely responsible for obtaining all necessary consents, licenses and approvals for the collection and Processing of any Personal Information/ Personal Data.

3. Technical, organizational measures and Security

3.1. Company implements and maintains appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The parties agree that the security measures as described in ANNEX II are appropriate to protect Personal Information/ Personal Data against a Security Incident, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Information/ Personal Data to be protected having regard to the state of the art and the cost of their 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. Taking into account any changes in the Processing activities, the risks and the applicable legal requirements, Company shall periodically review and update the security measures as described in ANNEX II to ensure ongoing compliance with this DPA and Data Protection Laws.

3.2. Company shall ensure that any person authorized to Process the Personal Information/ Personal Data is subject to a strict duty of confidentiality and that they Process the Personal Information/ Personal Data only for the purpose of delivering the Services under the Agreement to Customer.

3.3. At a minimum, Company agrees to maintain SOC2 Type 2 compliance and ISO 27001:2013 or equivalent standards, the scope of which contains the Security Measures identified at ANNEX II. Company may modify its Security Measures from time to time and at any time, provided, however, that it will not materially reduce the level of protection as provided in this DPA.

3.4. At all times that Company Processes, and/or has access to Personal Information/ Personal Data, Company shall (a) Process such Personal Information/ Personal Data only in accordance with Customer's documented instructions (unless Company is required by applicable laws or binding order of a governmental body responsible for the protection of Personal Information/ Personal Data in the relevant jurisdiction) (b) not Sell or Share (as defined under CCPA and CPRA, as applicable) Personal Information/ Personal Data, or retain, use, or disclose such Personal Information/ Personal Data (i) for any purpose other than for the specific purpose of performing the Services or (ii) outside the direct business relationship between Customer and Company.

3.5. Acknowledging that Customer (and not Company): (i) controls the nature and contents of Customer Data (including any Personal Information/ Personal Data therein); and (ii) acts as its own system administrator and controls user access to Customer Data (including any Personal Information/ Personal Data therein), Customer represents and warrants that on the date of this DPA and during the Term:

3.5.1. Personal Information/ Personal Data has been and will be collected and Processed by Customer in accordance with applicable Privacy/Data Protection Laws;

3.5.2. Customer will take all steps necessary to ensure it achieves the foregoing, including without limitation, by providing Data Subjects with appropriate privacy notices, obtaining any required consent, and ensuring that there is a lawful basis for Contracted Processors to Process Personal Information/ Personal Data.

4. Sub-Processing

4.1. If Customer and Company have entered into Standard Contractual Clauses as described in Section 5 (Cross-Border Transfers), (a) the authorizations in this DPA will constitute Customer's prior written consent to the subcontracting by Company of the Processing of Customer's Personal Data if such consent is required under the Standard Contractual Clauses, and (b) the parties agree that the copies of the agreements with Authorized Sub-processors that must be provided by Company to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that Company will provide such copies only upon request by Customer. Notwithstanding this, Customer consents to Company engaging (i) the Sub-processors listed in this section 4.1; and (ii) new Sub-processors provided that Company gives Customer reasonable prior notice which may be given by posting details of such addition (or the removal of a Sub-Processor) at the following url: <https://www.givingstep.com/legal>

Approved Company's Sub-Processors

Sub-Processor	Purpose	Location (By Country)
<i>Amazon Web Services ("AWS")</i> aws.amazon.com	Cloud hosting provider and translation assistance built into the TGS application	United States of America, Canada, United Kingdom, Australia, Singapore or European Union (per Customer election)
<i>Microsoft Azure</i> azure.microsoft.com	Cloud hosting provider, translation assistance and other AI services built into the TGS application	United States of America
<i>Google Cloud</i> cloud.google.com	Cloud hosting provider and translation assistance built into the TGS application	United States of America
<i>OpenAI</i> openai.com	Content writing assistance using generative AI with OpenAI's GPT AI	United States of America

4.2. If, within thirty (30) days of receipt of notice of a new Sub-Processor, Customer notifies Company in writing of any objections (on reasonable grounds relating to European Data Protection Laws) to the proposed appointment: Company shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-Processor; and where such a change cannot be made within thirty (30) days from Company's receipt of Customer's notice, notwithstanding anything in the Agreement, Customer may by written notice to Company with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-Processor.

4.3. Company shall (i) have executed a valid and enforceable written contract with the Sub-processor containing privacy and security provisions substantially similar to those contained in this DPA; (ii) Company remains fully liable for any Security Incident that is caused by an act, error or omission of such

Sub-processor; (iii) have put in place appropriate measures to ensure that international transfers of Personal Information/ Personal Data occur in compliance with Privacy/Data Protection Laws. Company shall verify and document the sufficiency of the safeguards provided by such Sub-processor taking into account the risk associated with the Processing activities and make available the information documented by Company on request by Customer.

5. Cross-Border transfers

5.1. The parties agree that when the transfer of Customer Personal Data from Customer to Company or a Company Affiliate is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

5.1.1. in relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

5.1.1.1. Module Two will apply to the extent that Customer is a Controller of the Customer Personal Data;

5.1.1.2. in Clause 7, the optional docking clause will apply;

5.1.1.3. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in section 4.1 of this Addendum;

5.1.1.4. in Clause 11, the optional language will not apply;

5.1.1.5. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

5.1.1.6. in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland.

5.1.1.7. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Addendum;

5.1.1.8. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Addendum; and

5.1.2. in relation to Customer Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

5.1.2.1. for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of personal data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("Prior C2P SCCs") for transfers of Customer Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the Customer on the one hand and Company or the applicable Company Affiliate on the other hand, on the following basis:

5.1.2.1.1. Appendix 1 shall be completed with the relevant information set out in Annex I to this Addendum;

5.1.2.1.2. Appendix 2 shall be completed with the relevant information set out in Annex II to this Addendum; and

5.1.2.2. the optional illustrative indemnification Clause will not apply.

5.1.3. Where Section 5.1.2.1 above does not apply, but the Customer and Company or the applicable Company Affiliate are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("UK Addendum") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

5.1.3.1 The EU SCCs, completed as set out above in section 5.1.1 of this Addendum shall also apply to transfers of such Customer Personal Data, subject to section 5.1.3.2 below;

5.1.3.2. The UK Addendum shall be deemed executed between the transferring Customer and Company or the applicable Company Affiliate, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Customer Personal Data.

5.1.4. If neither section 5.1.3.1 or section 5.1.3.2 applies, then the Customer and the Company or the applicable Company Affiliate shall cooperate in good faith to implement appropriate safeguards for transfers of such Customer Personal Data as required or permitted by the UK GDPR without undue delay.

5.1.5. In relation to Customer Personal Data that is protected by the Swiss FADP, the EU SCCs subject to the following modifications:

5.1.5.1 Any references in the EU Standard Contractual Clauses to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP;

5.1.5.2. References to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be;

5.1.5.3. References to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland, and

5.1.5.4 Unless the EU Standard Contractual Clauses, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss FADP, in which case the Swiss SCCs shall instead be incorporated by reference and form and integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant annexes or appendices of the Swiss SCCs shall be populated using the information contained in the Annexes to this DPA (as applicable).

5.2. Neither Company nor any Company Affiliate shall participate in (nor permit any Subprocessor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Customer Personal Data) unless the Restricted Transfer is made in full compliance with European Data Protection Laws and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Data.

5.3. The Parties agree that for the purposes of Restricted Transfers, each Secondary Customer and each Customer Affiliate shall be considered as a data exporter and that the provisions contained in this DPA apply to all Secondary Customers and Customer Affiliates as third-party beneficiaries if and to the extent the Company processes Customer Personal Information/ Personal Data for which the respective Secondary Customer or Customer Affiliate qualifies as Data Controller.

6. Deletion and Return

6.1 Upon Customer’s request, and subject to its customary data retention and archival processes, Company shall destroy all electronic Personal Information/ Personal Data or return to Customer all documented physical Personal Information/ Personal Data (including copies) in its possession or control (including any Personal Information/ Personal Data Processed by its Sub-Data Processors). This requirement shall not apply to the extent that Company is required by any Privacy/Data Protection Laws to retain some or all of the Personal Information/ Personal Data, in which event Company will isolate and protect the Personal Information/ Personal Data from any further Processing except to the extent required by such Privacy/Data Protection Laws. Electronic copies of Personal Information/ Personal Data stored in computer system backups that cannot reasonably be isolated for deletion from the backup and that are retrievable only by using special tools need not be returned or destroyed provided that access to the system backup is restricted and the Personal Information/ Personal Data is held in confidence for so long as Company’s obligations under this Agreement continue.

7. Cooperation

7.1. To the extent Company is required under Privacy/Data Protection Laws, Company will assist Customer to comply with Privacy/Data Protection Laws; in particular (i) Company will assist Customer in responding to any request from a data subject exercising his or her rights under the Privacy/Data Protection Laws; (ii) it will assist Customer in responding to any request from regulatory or judicial bodies relating to the Processing of Personal Information/ Personal Data under the Agreement(s); (iii) it will promptly notify Customer if its Processing of Personal Information/ Personal Data is likely to result in a high risk to the privacy rights of data subjects or is unable to comply with Customer’s instructions for any reason, (iv) upon reasonable request, will assist Customer to carry out data protection impact assessments, and (v) upon reasonable request, will assist Customer to carry out transfer impact assessments and identify any supplementary measures appropriate to any Restricted Transfer carried out in accordance with Section 5 of this DPA, where relevant.

8. Security Incidents

8.1. If Company becomes aware of a Security Incident or has a reasonable suspicion of a Personal Information/ Personal Data breach in respect of the Personal Information/ Personal Data being Processed under the Agreement(s), it will inform Customer without undue delay and will provide reasonable information and cooperation to Customer so that Customer can fulfil any Personal Information/ Personal Data Security Incident reporting obligations it may have under the applicable Privacy/Data Protection Laws. Company will

take reasonably necessary measures to remedy and mitigate the effects of the Security Incident and will keep Customer informed of all material developments with the Security Incident.

8.2. Insofar as it relates to Customer, the content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Customer's discretion, except as otherwise required by Privacy/Data Protection Laws.

9. Data Protection Impact Assessment and Prior Consultation

9.1. At Customer's request, Company shall provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with Supervisory Authorities or other competent data privacy authorities, as required by Article 35 or 36 of the GDPR, and in each case solely in relation to Processing of Personal Data by and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Audit Reports and Inspections

10.1 Audit Reports. Information and audit rights of Customer under Clause 16 of the Agreement apply in relation to Personal Information/Personal Data whose Processing is subject to the certain Data Protection/Privacy Laws.

11. Severance

11.1 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12. Governing Law

12.1. Except as provided in Section 5.1.1.5, the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity, or termination or the consequences of its nullity; and

12.2. Except as provided in Section 5.1.1.6, this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

12.3. The obligations placed under this DPA shall survive so long as Company and/or its Sub-processors Processes Personal Information/ Personal Data on behalf of Customer.

12.4. This DPA may not be modified except by written instrument signed by both parties. If any part of this DPA is held unenforceable, the validity of all remaining clauses will not be affected.

12.5. In the event of any conflict between this DPA and the Agreement(s), the terms of this DPA shall prevail.

Annex I

Data Processing Description

This Annex I forms part of the Addendum and describes the Processing that Company and Company Affiliates will perform on behalf of the Customer.

A. LIST OF PARTIES

Controller(s) / Data exporter(s):

Name:	The entity identified in the Agreement and/or Order Form(s)/Statement(s) of Work and all Affiliates of Customer established within the European Economic Area (EEA), the United Kingdom, and/or Switzerland.
Address:	The Customer's address, as set out in the Agreement, and/or Order Form(s)/Statement(s) of Work
Contact person's name, position and contact details:	Customer's telephone number and email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work
Activities relevant to the data transferred under these clauses:	The purchase of Services as set out in the Agreement
Signature and date:	This Annex I shall be deemed signed and effective as of the date of the Agreement and/or Order Form/Statement of Work of which it forms part.
Role (controller/processor):	Controller

Processor(s) / Data importer(s):

Name:	The Giving Step, LLC for itself and its Affiliates, located outside EEU/EEA, the United Kingdom and/or Switzerland
Address:	117 Marions Oak Dr. Summerville SC 29486
Contact person's name, position and contact details:	Name: Donald Swope Position: VP of Technology Contact Details: info@thegivingstep.com
Activities relevant to the data transferred under these Clauses:	The provision of services as set out in the Agreement
Signature and date:	This Annex I shall be deemed signed with and effective as of the date of the Agreement and/or Order Form/Statement of Work of which it forms a part.
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Employees, Prospects and/or Customers, and Contractors.
Categories of personal data transferred:	First name, last name, work email address, job title, cookie ID, log data, password, IP address.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	N/A
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Check as applicable: A one-off transfer: ☐ Occurring on a continuous basis for the length of the Agreement: x Another frequency (if yes, give details): ☐
Nature and purposes of the transfer and processing:	The data exporter will transfer Customer Personal Data for the purposes of the provision of services by Company to the data exporter as described in the Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Customer Personal Data will be retained for the period in which services are provided under the Agreement. The criteria used to determine that period will be based on the purposes for which the data is processed, and any period required to meet legal obligations or to exercise, defend or establish legal rights.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As described above, Company (as data importer) will process Customer Personal Data (as described above) for the purposes of the provision of services to the data exporter as described in the Agreement. The duration of the processing will be as described above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	For Personal Data protected under the EU GDPR: Where the data exporter is established in the EEA, the competent supervisory authority shall be the lead supervisory authority for the data exporter. Where the data exporter is not established in the EEA but has appointed an EU representative, this shall be the supervisory authority for the territory in which the EU representative is established. In all other cases, the Irish Data Protection Commission shall be deemed the competent supervisory authority for these Standard Contractual Clauses. For Personal Data protected under the UK GDPR: Information Commissioner's Office. For Personal Data protected under the Swiss FAPD: the Swiss Federal Data Protection and Information Commission.
---	--

Annex II

Technical and Organizational

Security Measures

Description of the technical and organizational measures implemented by the processor(s) / 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.

Measure	Description
Measures of pseudonymisation and encryption of personal data	All data is encrypted with volume level encryption using 256-bit Advanced Encryption Standard (AES-256) in Galois/Counter Mode, known as AES-GCM, and all Personal Data is pseudonymized.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Company shall ensure that any person authorized to Process the Personal Information/ Personal Data is subject to a strict duty of confidentiality and that they Process the Personal Information/ Personal Data only for the purpose of delivering the Services under the Agreement to Customer. All systems are backed up regularly with failover systems/processes in place.
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	Global and redundant service infrastructure, resilient backup technology and processes in place to test our capability to restore Customer data.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Company maintains an ISO 27001:2013 certification and is audited for SOC 2 Type 2 compliance annually.
Measures for user identification and authorization	Appropriate access control is maintained to Company systems and Customer Data is highly protected in line with our data classification and treatment policies. Employees who have elevated level of access are required to undertake mandatory information security awareness training. All users are required to use named accounts and access to systems and data is logged.
Measures for the protection of data during transmission	Personal Information/ Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys or is transferred over private network connectivity.
Measures for the protection of data during storage	TGS data at rest encryption uses one of the strongest block ciphers available – 256-bit Advanced Encryption Standard (AES-256). Every protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. The mechanism provides additional security by storing the encrypted data and encryption keys in different hosts.
Measures for ensuring events logging	Company's auditing and logging standards are modeled after the National Institute of Standards and Technology (NIST)'s Special Publication Guide to Computer Security Log Management (SP 800-92).
Measures for internal IT and IT security governance and management	Company's Information Security Management System is implemented per ISO 27001 family of standards and framework. Additionally, Company is audited annually for SOC 2 Type 2 compliance.
Measures for ensuring data minimization	Company only processes the minimum amount of Personal Data needed in order to carry out its obligations under the Agreement.
Measures for ensuring limited data retention	Data is backed up continuously and is retained on a rolling 12-month cycle.

Measures for allowing data portability and ensuring erasure]	Company has appropriate methods in place to allow users to transmit personal data in structured, commonly used and machine-readable format. This is available through self service functions in the Software. Users may also request their data through our support service. Further, Company has processes and procedures to receive, recognize, record, and respond to right to erasure or right to be forgotten requests, provided they do not conflict with contractual obligations, and/or applicable law.
--	---