Outreach Privacy and Security Addendum

This Outreach Privacy and Security Addendum ("**Addendum**"), is made part of and is incorporated by reference into the current applicable Order(s) and/or Master Service Agreement or equivalent agreement for Outreach Services ("**Agreement**") between Outreach Corporation ("**Outreach**") and the customer entity identified in the Agreement ("**Customer**") (each referred to as a "**Party**" and collectively as the "**Parties**").

This Addendum will be effective, and will supersede and replace in its entirety any existing data processing addendum the parties may have previously entered into in connection with the Outreach Services, from the date on which Customer signed the Agreement ("**Effective Date**").

RECITALS

This Addendum governs the manner in which Outreach shall process Customer Personal Data (as defined below) and only applies to the extent Outreach Processes such Customer Personal Data in its role as a data processor. Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. In the event of a conflict between the Agreement, including Orders and Exhibits, and this Addendum, the provision imposing the stricter data protection requirements of any conflicting provision shall control. Capitalized terms have the meaning given to them in the Agreement, unless otherwise defined below.

1. Definitions

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Applicable Data Protection Law(s)**" means the relevant data protection and data privacy laws, rules and regulations applicable to the Processing of Customer Personal Data under this Addendum including any binding laws or regulations ratifying, implementing, adopting, supplementing or replacing the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

b) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

c) "**Customer Personal Data**" means Personal Data that Outreach Processes in its role as a data processor (or any substantially similar terms) under Applicable Data Protection Laws , as further specified in Schedule 1.

d) "**Instructions**" means Customer's instructions to Outreach directing Outreach to process the Customer Personal Data as provided to Customer under the Agreement, this Addendum and applicable Order Form, or through Customer's use of the features and functionality of the Services or as otherwise mutually agreed by both parties in writing.

e) "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

f) "**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

g) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data subject to this Addendum.

h) "**Security Incident(s)**" means (i) a breach in security leading to any unauthorized interference with the availability of, or any unauthorized, unlawful or accidental access or damage to or loss, misuse, destruction, alteration, acquisition, disclosure of, Customer Personal Data that may adversely affect the privacy or security of individuals or Customer Personal Data; or (ii) as otherwise defined under Applicable Data Protection Laws. Security Incidents do not include unsuccessful attempts or activities that do not compromise the confidentiality, availability, or integrity of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other similar incidents.

i) "**Sensitive Personal Data**" shall have the meaning assigned to the terms "sensitive data", "sensitive information", "special categories of personal data", or similar term under Applicable Data Protection Law(s) and, as required by Applicable Data Protection Law(s), shall include Customer 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 data concerning a natural person's sex life or sexual orientation.

j) "**Standard Contractual Clauses**" means the (i) the standard contractual clauses for international transfers published by the European Commission on June 4, 2021 governing the transfer of European Area Personal Data to Third Countries as adopted by the European Commission, and the Swiss Federal Data Protection and Information Commissioner ("**Swiss FDPIC**") relating to data transfers to Third Countries (collectively "**EU SCCs**"); (ii) the international data transfer addendum ("**UK Transfer Addendum**") adopted by the UK Information Commissioner's Office ("**UK ICO**") for data transfers from the UK to Third Countries; or (iii) any similar such clauses (as applicable) adopted by a data protection regulator relating to data transfers to Third Countries, including without limitation any successor clauses thereto.

k) "**Sub-processor(s)**" means Outreach authorized contractors, agents, vendors and third party service providers that Process Customer Personal Data.

l) **"Third Country"** means countries that, where required by Applicable Data Protection Laws, have not received an adequacy decision from an applicable authority relating to data transfers, including regulators such as the European Commission, UK ICO, or Swiss FDPIC relating to data transfers.

2. Data Handling and Access

a) Role of the Parties. The parties acknowledge and agree that with respect to Processing of Customer Personal Data, Outreach is a Processor and Customer is a Controller and/or a Processor in which case Outreach is a sub-processor.

b) General Compliance by Outreach. Customer Personal Data shall be Processed by Outreach in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

c) General Compliance by Customer. Customer represents and warrants that (i) it shall comply with its obligations under Applicable Data Protection Law(s) in respect of its Processing of Customer Personal Data and any Processing Instructions it issues to Outreach and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Applicable Data Protection Law(s) for Outreach to Process Customer Personal Data and provide the Outreach Services pursuant to the Agreement and this Addendum.

d) Outreach and Sub-processors. Outreach agrees to (i) enter into a written agreement with Sub-processors regarding such Sub-processors' Processing of Customer Personal Data that imposes on such Sub-processors data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Outreach's Sub-processors' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.

e) Authorization to Use Sub-processors. Customer authorizes Outreach to use the Sub-processors described in Schedule 3. If Outreach engages new Sub-processors, Outreach will give Customer notice at least 30 calendar days in advance of providing that Sub-processor with access to Customer Personal Data. If Customer does not approve of a new Sub-processor on reasonable data protection grounds, Customer may terminate the applicable Order without penalty by providing, within 30 calendars days of notice of such new Sub-processor, written notice of termination that includes an explanation of the grounds for non-approval. Where Outreach engages a Sub-processor for carrying out specific processing activities on behalf of Customer, the same (or substantially similar) data protection obligations as set out in this Addendum shall be imposed on that Sub-processor by way of a written agreement. Where that Sub-processor fails to fulfil its data protection obligations, Outreach shall remain fully liable to Customer for the performance of its Sub-processor obligations.

f) Following Instructions. Outreach shall Process Customer Personal Data only in accordance with Customer's Instructions. Outreach will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's Instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's Instructions.

g) Confidentiality. Any person authorized to Process Customer Personal Data on behalf of Outreach must be under an appropriate statutory or contractual obligation of that requires such person to maintain the confidentiality of the Customer Personal Data.

h) Personal Data Inquiries and Requests. Outreach agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Applicable Data Protection Law(s) ("**Privacy Request**"). At Customer's request and without undue delay, Outreach agrees to assist Customer in answering or complying with any Privacy Request. The obligations under this provision shall apply solely where and to the extent required by Applicable Data Protection Law.

i) Processing of Sensitive Personal Data. Customer will not submit sensitive personal data to the Outreach Services without written consent from Outreach or agreement from Outreach to enter into a business associate agreement. In such cases, the parties acknowledge that limited special categories of personal data may incidentally be entered by Customer through Customer's use of the Services in the regular course of business.

j) Sale of Customer Personal Data Prohibited. Outreach shall not sell or share Customer Personal Data as such terms are defined under the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) or any substantially similar law, nor use, retain, or disclose Customer Personal Data outside of its direct business relationship with the Customer or for any other purpose except as required or permitted by such law.

k) Prior Consultation. Where and to the extent required by Applicable Data Protection Law, Outreach agrees to provide reasonable assistance at Customer's expense to Customer where (i) in Customer's reasonable judgement, the type of Processing performed by Outreach is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling; (ii) Processing Sensitive Personal Data on a large scale and systematic monitoring on a large scale; or (iii) where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

l) Demonstrable Compliance. Where and to the extent required by Applicable Data Protection Law, Outreach agrees to keep records of its Processing of Customer Personal Data and provide such records to Customer upon reasonable request to assist Customer with complying with supervisory authorities' requests.

m) Notice of Non-Compliance. Where and to the extent required by Applicable Data Protection Law, Outreach shall promptly notify Customer's Designated POC (as defined below) if it can no longer meet its obligations under this Addendum.

3. International transfers

a) Onward Transfers. In connection with the provision of the Services to Customer, Outreach may (and may authorize its Sub-processors to) receive or transfer and Process Customer Personal Data from any country to Third Countries provided that Outreach and its Sub-processors take measures to adequately protect such data consistent with Applicable Data Protection Laws. Such measures may include to the extent available and applicable under such laws:

i) *Standard Contractual Clauses***.** The parties' agreement to enter in to and comply with the Standard Contractual Clauses which are hereby incorporated into this Addendum and as further set forth in Schedule 1 and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Applicable Data Protection Laws; or

ii) *Other Approved Transfer Mechanisms*. Implementing any other data transfer mechanisms or certifications approved under Applicable Data Protection Laws, including, as applicable, any approved successor or replacement to the EU–US Privacy Shield framework, the Swiss–US Privacy Shield framework.

To the extent that any substitute or additional appropriate safeguards or mechanisms under any Applicable Data Protection Laws are required to transfer data to a Third Country the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this Addendum.

b) European Cross-Border Data Transfer Mechanisms.

i) *European Personal Data Transfers*. Transfers of Customer Personal Data from the European Union, European Economic Area, Switzerland, or the United Kingdom of Great Britain and Northern Ireland ("**UK**") by Customer to Outreach or Outreach to Customer in Third Countries are subject to the Standard Contractual Clauses, Module Two ("**Controller to Processor**"), and Module Three ("**Processor to Processor**") attached to this Addendum and incorporated by reference. The information required for the purposes of the Standard Contractual Clauses is provided in Schedule 1 ("Description of Processing and Transfer Details") to this Addendum. The Parties agree that the Standard Contractual Clauses are incorporated into this Addendum without further need for reference, incorporation, or attachment and that by executing this Addendum, each party is deemed to have executed the Standard Contractual Clauses.

ii) *Swiss Personal Data Transfers*. For international transfers of Customer Personal Data subject to Applicable Data Protection Laws in Switzerland, the Standard Contractual Clauses shall be read to be modified as follows as applicable:
(1) References to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the Swiss FDPIC.
(2) References to "EU", "Union" and "Member State" shall be interpreted to include references to "Switzerland".

iii) *UK Personal Data Transfers*. For international transfers of Customer Personal Data subject to Applicable Data Protection Laws in the United Kingdom and transferred in accordance with the UK Transfer Addendum, the Parties agree as follows:
(1) Each Party agrees to be bound by the terms and conditions set out in the UK Transfer Addendum, in exchange for the other Party also agreeing to be bound by the UK Transfer Addendum.
(2) The Standard Contractual Clauses will be interpreted in accordance with Part 2 of the UK Transfer Addendum.
(3) Sections 9 to 11 of the UK Transfer Addendum override Clause 5 (Hierarchy) of the EU SCCs
(4) For the purposes of Section 12 of the UK Transfer Addendum, the EU SCCs will be amended in accordance with Section 15 of the UK Transfer Addendum.
(5) Information required by Part 1 of the UK Transfer Addendum is provided as Schedule 1 to this Addendum
(6) To the extent that any revised transfer addendums or mechanisms are issued by the UK ICO, the Parties agree to incorporate such revisions in accordance with Section 18-20 of the UK Transfer Addendum.

4. Information Security Program

Outreach agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s). Such measures shall include security measures equal to, or better than, those specified in Schedule 2. Customer has reviewed such measures and acknowledges that they are appropriately designed to ensure a level of security appropriate to the risks that are presented by the Processing of Customer Personal Data under this Addendum. Further, Outreach agrees to regularly test, assess and evaluate the effectiveness of its technical and organizational measures to ensure the security of the Processing. Outreach has comprehensive privacy and security assessments and certifications performed by multiple third parties. Such certifications include SOC 2, ISO 27001: 2013, and TRUSTe, details of which can be found at https://www.outreach.io/trust/.

5. Audits

Upon Customer's request and no more than once per calendar year, Outreach shall make available for Customer's review copies of certifications or reports demonstrating Outreach compliance with Applicable Data Protection Laws as they relate to the processing of Customer's Personal Data.

6. Return or Deletion of Data

Upon termination of the provision of the Outreach Services, Outreach shall within sixty (60) days, or any other applicable destruction period set forth in the Agreement, whichever is longer, destroy, or, at Customer's request, return the Customer Personal Data.

Outreach may retain Customer Personal Data to the extent that it is required or authorized to do so under applicable law and/or regulation or to the extent Customer Personal Data is archived on Outreach's back-up systems, in which case Outreach will securely isolate and protect such data from any further processing, except to the extent required by applicable law and/or regulation.

7. Security Incident

a) Security Incident Procedure. Outreach will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b) Notice. Outreach agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) to Customer's Designated POC if it knows or suspects that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

8. Contact Information

Outreach and the Customer agree to designate a point of contact for urgent security issues (a "**Designated POC**"). The Designated POC for both parties are:

- Outreach Designated POC: security@outreach.io
- Customer Designated POC: as identified in Agreement

Schedule 1 to the Addendum

Description of Processing and Transfer Details

1. Data Exporter

Company Name	Address	Contact name, position, and contact information	Role
Customer information as included in the applicable Order Form			Controller

2. Data Importer

Company Name	Address	Contact name, position, and contact information	Role
Outreach Corporation	333 Elliott Ave W, Suite 500 Seattle, WA 98119	privacy@outreach.io	Processor

3. Activities relevant to the data transferred under the SCCs

The activities relevant to the data transferred at the Services more fully described in the Agreement and applicable Orders.

4. Details of Customer Personal Data

Categories of data subjects whose personal data is transferred	Includes the following: • Prospects, customers, business partners and vendors of Customer (who are natural persons) • Employees or contact persons of Customer's prospects, customers, business partners and vendors • Employees, agents, advisors, freelancers of Customer (who are natural persons) • Customer's users authorized by Customer to use the Outreach Services
Categories of personal data transferred	Includes the following: • Identification Data (notably email addresses, usernames and phone numbers) • Electronic identification data (notably IP addresses and mobile device IDs)
Sensitive Personal Data transferred	Customer will not submit Sensitive Personal Data to the Outreach Services without written consent from Outreach or agreement from Outreach to enter into a business associate agreement. In such cases, the parties acknowledge that limited special categories of personal data may incidentally be entered by Customer through Customer's use of the Services in the regular course of business.
Frequency of the transfer	Continuous
Nature and purpose of the data transfer and further processing	The purpose of Processing of Customer Personal Data by Outreach is the performance of the Outreach Services pursuant to the Agreement.
Period for which the personal data will be retained or criteria used to determine that period	The period for which the personal data will be retained is more fully described in the Agreement, Addendum, and accompanying Order Forms.

Subprocessor transfers – subject matter, nature, and duration of processing	The subject matter, nature, and duration of the Processing as more fully described in the Agreement, Addendum, and accompanying Order Forms.

-

5. Signatures

Signatures	The Parties agree that the EU SCCs and the UK Transfer Addendum are incorporated by reference and that by executing the Addendum, each party is deemed to have executed the SCCs and the UK Transfer Addendum.

6. European Area SCC and UK Transfer Addendum Information

SCC Clause	**GDPR**	**Swiss DPA**	**UK Data Protection Law**
Module in Operation: Module Two (Controller to Processor) and Module Three (Processor to Processor)			
Clause 7- Docking Clause	An entity that is not a party to these Standard Contractual Clauses may, with the agreement of the parties, accede to these Standard Contractual Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A of the Standard Contractual Clauses.		
Clause 9(a)- Use of Sub-processors	**GENERAL WRITTEN AUTHORISATION**: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 calendar 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.		
Clause 11 (Redress)	Optional language in Clause 11 shall not apply.		
Clause 17- Governing Law	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.
Clause 18 – Choice of Forum and Jurisdiction	(b) The parties agree that those shall be the courts of Ireland.	The parties agree that those shall be the competent courts of Switzerland.	The parties agree that those shall be the competent courts of England and Wales.
Annex 1A- List of Parties	The name, address, and contact person's name, position, and contact details, and each party's role in processing Customer Personal Data are provided in Section 1, 2, and 3 above		
Annex 1B – Description of Transfer	This information can be found in Section 4 above.		
Clause 13 and Annex 1C – Competent Supervisory Authority	Identify the competent supervisory authority/ies in accordance with Clause 13: Irish Data Protection Commission	Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	Identify the competent supervisory authority/ies in accordance with Clause 13: UK Informational Commissioner
Annex II – Technical and Organizational Measures	The description of technical and organization measures designed to ensure the security of Customer Personal Data is described more fully in Schedule 2 of this Addendum.		

Annex III – List of Subprocessors	See Schedule 3 of this Addendum.	
Ending the UK Transfer Addendum when the Approved Addendum changes	**N/A**	Which Parties may end this Addendum as set out in Section 19: ☒Importer ☒Exporter ☐neither Party

Schedule 2 to the Addendum

Outreach Information Security Controls

Measures for:	Descriptions
pseudonymisation and encryption of personal data	Implement and maintain modern and industry standard encryption mechanism and pseudonymize data as applicable to the Services provided.
ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Implement and maintain a formal information security program that considers the ongoing confidentiality, integrity, availability, and processing of systems.
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	Implement and maintain measures to ensure the availability of data according to agreed-upon RTO and RPO. Measures should include backup procedures, geographical separation, and redundancy.
regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Implement a review program for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures using a risk-based approach (risk assessment and internal audit) and periodically by a qualified third party (external and penetration test). Mitigation and remediation actions required based on the results of such testing, should be documented and executed in a timely manner.
user identification and authorisation	Implement and maintain mechanisms for establishing identity and accountability including unique ID, strong password, and multifactor authentication.
the protection of data during transmission	Implement and maintain industry standard encryption protocols for encrypting data in transit, including but not limited to logins and sensitive data transfers.
the protection of data during storage	Implement and maintain industry standard encryption protocols for encrypting data at rest.
ensuring physical security of locations at which personal data are processed	Implement and maintain physical security measures for locations used for data processing and storage.
ensuring events logging	Implement and maintain controls around logging, monitoring, and alerting based on pre-defined thresholds.
ensuring system configuration, including default configuration	Implement and maintain a formal hardening standard to ensure that configurations of system align with NIST, ISO, or equivalent guidance.
internal IT and IT security governance and management	Implement and maintain measures to ensure that IT policy and control are established and communicated, understood, and acknowledged throughout the organization.
certification/assurance of processes and products	Implement and maintain external certification and attestation of systems and controls used to secure the process information relevant to the services provided (SSAE 18/SOC 2, ISO 27701, ISO 27001, External Pen test, etc.)
ensuring data minimisation	Implement and maintain controls to limit data collected through the Services provided and limit the use of data to the agreed upon uses or for providing the Services.
ensuring data quality	Implement and maintain controls to maintain the accuracy, completeness, and consistency of data over its life cycle.
ensuring limited data retention	Implement and maintain controls for deleting data according to request or agreed upon terms of retention post termination of the agreement.
ensuring accountability	Implement and maintain measures to ensure accountability and responsibility for security, privacy, and breach notification.
allowing data portability and ensuring erasure	Implement and maintain measures to allow for portability of data and ensuring complete erasure upon request or contract term.
transfers to (sub-) processors, also describe the specific technical and organizational 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:	Outreach remains committed to provide commercially reasonable cooperation and assistance to controllers. As set forth in the Addendum, Outreach will delete or return Customer Personal Data in accordance with the prior written instructions of the Customer. In addition, upon request, Outreach will, to the extent not prohibited by law, reasonably assist the Customer in responding to any data subject request. Further, when Outreach engages a sub-processor pursuant to the Addendum, Outreach is required to first enter into an agreement with such sub-processor that contains data processing obligations substantially similar to those contained in the Addendum.

Schedule 3 to the Addendum

SUB-PROCESSORS

The following list identifies the Sub-processors of Outreach authorized to Process Customer Personal Data as further specified in Section (e) of the Addendum: https://www.outreach.io/sub-processors.