Data Processing Agreement

Effective: April 10, 2022

Scope of Data Processing Agreement

This Data Processing Agreement ("DPA") is incorporated into, and is subject to the terms and conditions of, the Agreement between Reach Security, Inc. (together with its Affiliates, "Reach Security") and the customer entity that is a party to the Agreement ("Customer" or "you").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA (including the SCCs (where applicable), as defined herein).

1. Definitions.

"Agreement" means the written agreement between Customer and Reach Security which governs the provision of the Service to Customer, as such terms or agreement may be updated from time to time.

"Control" has the meaning set forth in the Agreement. The term "Controlled" shall be construed accordingly.

"Customer Data" means any personal data that Reach Security processes on behalf of Customer via the Service, as more particularly described in this DPA.

"Data Protection Laws" means all data protection laws and regulations applicable to a party and/or the processing of Customer Data under the Agreement, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.

"EU Data Protection Law" means (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (in each case, as may be amended, superseded or replaced).

"Europe" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"SCCs" means the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

"Security Incident" means any unauthorized or unlawful breach of security that leads to, or is reasonably believed to have led to, the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by Reach Security.

"Sensitive Data" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

"Sub-processor" means any processor engaged by Reach Security, including its Affiliates, to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Reach Security but shall exclude Reach Security employees, individual contractors, or individual consultants.

The terms "personal data", "controller", "data subject", "processor" and "processing" shall have the meaning given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and "process", "processes" and "processed", with respect to any Customer Data, shall be interpreted accordingly.

2. Roles and Responsibilities

2.1 *Parties' roles.* The parties acknowledge and agree that with regard to the processing of Customer Data, Customer is the controller and Reach Security is a processor acting on behalf of Customer, as further described in Annex A (Details of Data Processing) of this DPA. For the avoidance of doubt, this DPA shall not apply to instances where Reach Security is the controller (as defined by EU Data Protection Law) unless otherwise described in Annex D hereto.

2.2 *Purpose limitation.* Reach Security shall at all times process Customer Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing ("Permitted Purposes"). The parties agree that the Agreement sets out Customer's complete and final instructions to Reach Security in relation to the processing of Customer Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 *Prohibited data.* Customer will not provide (or cause to be provided) any Sensitive Data to Reach Security for processing under the Agreement, and Reach Security will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.4 *Customer compliance.* Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Reach Security; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Reach Security to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

2.5 *Compliance with Data Protection laws.* Each Party will ensure that its processing of the Customer Data in accordance with the Agreement will not cause the other Party to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws

3. Sub-processing

3.1 *Authorized Sub-processors.* Customer consents to Reach Security engaging the Sub-processors set forth in our list of Subprocessors. Reach Security shall notify Customer if it adds or removes Sub-processors at least 10 days prior to any such changes. Customer may opt-in to receive such notifications by emailing a request to support@reach.security.

3.2 *Sub-processor obligations.* Reach Security shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Reach Security to breach any of its obligations under this DPA.

3.3 *Objection to Sub-processors.* Customer may object in writing to Reach Security' appointment of a new Sub-processor on reasonable grounds relating to data protection by notifying Reach Security promptly in writing within five (5) calendar days of receipt of Reach Security' notice. Such notice shall explain the reasonable grounds for the objection. In such an event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If this is not possible, either party may terminate the applicable Services that cannot be provided by Reach Security without the use of the objected-to-new Sub-processor.

4. Security

4.1 *Security Measures.* Reach Security shall implement and maintain appropriate technical and organizational security measures that are designed to protect Customer Data from Security Incidents and designed to preserve the security and confidentiality of Customer Data in accordance with Reach Security's security standards described in Information Security Policy ("Security Measures").

4.2 *Confidentiality of Processing.* Reach Security shall ensure that any person who is authorized by Reach Security to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 *Updates to Security Measures.* Customer is responsible for reviewing the information made available by Reach Security relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Reach Security may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

4.4 *Security Incident response.* Upon becoming aware of a Security Incident, Reach Security shall: (i) notify Customer without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Reach Security's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Reach Security of any fault or liability with respect to the Security Incident.

4.5 *Customer responsibilities.* Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Service.

5. Security Reports and Audits

5.1 *Audit rights.* Reach Security shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5.1 and where applicable, the SCCs) and any audit rights granted by Data Protection Laws, by instructing Reach Security to comply with the audit measures described in Sections 5.2 and 5.3 below.

5.2 *Security reports.* Customer acknowledges that Reach Security is regularly audited by independent third-party auditors and internal auditors respectively. Upon written request, Reach Security shall supply (on a confidential basis) a summary copy of its most current audit report(s) ("Report") to Customer, so that Customer can verify Reach Security's compliance with the audit standards against which it has been assessed.

5.3 *Security due diligence*. In addition to the Report, Reach Security shall respond to all reasonable requests for information made by Customer to confirm Reach Security's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to infosec@reach.security, provided that Customer shall not exercise this right more than once per calendar year.

6. International Transfers

6.1 Data center locations. Subject to Section 6.2, Customer acknowledges that Reach Security may transfer and process Customer Data to and in the United States and anywhere else in the world where Reach Security, its Affiliates or its Sub-processors maintain data processing operations. Reach Security shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

6.2 *Australian data*. To the extent that Reach Security is a recipient of Customer Data protected by the Australian Privacy Law, the parties acknowledge and agree that Reach Security may transfer such Customer Data outside of Australia as permitted by the terms agreed upon by the parties and subject to Reach Security complying with this DPA and the Australian Privacy Law.

6.3 *European Data transfers.* To the extent that Reach Security is a recipient of Customer Data protected by EU Data Protection Laws ("EU Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for personal data (as described in applicable EU Data Protection Law), the parties agree to the following:

6.3.1 *SCCs:* Reach Security agrees to abide by and process EU Data in compliance with the SCCs in the form set out in Annex C. For the purposes of the descriptions in the SCCs, Reach Security agrees that it is the "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be an entity located outside Europe).

6.4 *Alternative transfer mechanism.* To the extent Reach Security adopts an alternative data export mechanism (including any new version of or successor to the SCCs) for the transfer of EU Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable EU Data Protection Law and extends to the countries to which EU Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data (within the meaning of applicable EU Data Protection Law), Reach Security may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of EU Data.

7. Return or Deletion of Data

Upon deactivation of the Services or request, Customer Data shall be deleted, save that this requirement shall not apply to the extent Reach Security is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which such Customer Data Reach Security shall securely isolate and protect from any further processing, except to the extent required by applicable law.

8. Data Subject Rights and Cooperation

8.1 *Data subject requests*. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Reach Security shall (at Customer's expense) taking into account the nature of the processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Reach Security, Reach Security shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Reach Security is required to respond to such a request, Reach Security shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 *Data protection impact assessment*. To the extent Reach Security is required under Data Protection Law, Reach Security shall (at Customer's expense) provide reasonably requested information regarding Reach Security's processing of Personal Data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. Jurisdiction-Specific Terms.

To the extent Reach Security processes Customer Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex D, then the terms specified in Annex D with respect to the applicable jurisdiction(s) ("Jurisdiction-Specific Terms") apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms' applicability to Reach Security.

10. Limitation of Liability

10.1 Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.2 Any claims made against Reach Security or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. Relationship with the Agreement

11.1 This DPA shall remain in effect for as long as Reach Security carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7.1 above).

11.2 The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service.

11.3 In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement.

11.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

11.6 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Annex A – Details of Data Processing

1. Controller (data exporter): Customer has engaged Reach Security to provide the Service to Customer in accordance with the Agreement.
2. Processor (data importer): Reach Security Inc, a Delaware corporation
3. Subject matter: The subject matter of the data processing under this DPA is the Customer Data.
4. Duration of processing: Reach Security will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.
5. Purpose of processing: Reach Security shall only process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement.
6. Nature of the processing: Reach Security provides a security platform and other related services, as more particularly described in the Agreement.
7. Types of Customer Data: Customer may upload, submit or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion.
8. Sensitive Data: Reach Security does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service.
9. Processing Operations: Customer Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: 9.1 Storage and other processing necessary to provide, maintain and improve the Service provided to Customer pursuant to the Agreement; and/or
10. 9.2 Disclosures in accordance with the Agreement and/or as compelled by applicable law.

Annex B – Security Measures

The Security Measures applicable to the Service are described in the Information Security Policy (as updated from time to time in accordance with Section 4.3 of this DPA).

Annex C - Standard Contractual Clauses

Standard Contractual Clauses

Annex D - Jurisdiction-Specific Terms

Europe:

1. Objection to Sub-processors. Customer may object in writing to Reach Security's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Reach Security will, at

its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

2. Government data access requests. As a matter of general practice, Reach Security does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Reach Security accounts (including Customer Data). If Reach Security receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about a Reach Security account (including Customer Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, Reach Security shall: (i) inform the government agency that Reach Security is a processor of the data; (ii) attempt to redirect the agency to request the data directly from Customer; and (iii) notify Customer via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy. As part of this effort, Reach Security may provide Customer's primary and billing contact information to the agency. Reach Security shall not be required to comply with this paragraph 2 if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or Reach Security's property, Sites, or Service.

UK:

1. For the avoidance of doubt, when European Union law ceases to apply to the UK upon the UK's withdrawal from the European Union and until such time as the UK is deemed to provide adequate protection for personal data (within the meaning of applicable EU Data Protection Law) then to the extend Reach Security processes (or causes to be processed) any Customer Data protected by EU Data Protection Law applicable to EEA and Switzerland in the United Kingdom, Reach Security shall process such Customer Data in compliance with the SCCs or any applicable Alternative Transfer Mechanism implemented in accordance with Section 6.3 and 6.4 of this DPA.

California:

1. Except as described otherwise, the definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA.
2. For this "California" section of Annex D only, "Reach Security Services" means the security tools and insights available for Reach Security Customers to use as may be further described in the Agreement and/or on the Reach Security website.
3. For this "California" section of Annex D only, "Permitted Purposes" shall include processing Customer Data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for "service providers" under the CCPA.
4. Reach Security's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, apply to Consumer's rights under the CCPA.
5. Notwithstanding any use restriction contained elsewhere in this DPA, Reach Security shall process Customer Data only to perform the Reach Security Services, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, except where otherwise required by applicable law.
6. Reach Security may de-identify or aggregate Customer Data as part of performing the Service specified in this DPA and the Agreement.
7. Where Sub-processors process the personal data of Customer contacts, Reach Security shall ensure that such Sub-processors are Service Providers under the CCPA with whom Reach Security has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale". Reach Security conducts appropriate due diligence on its Sub-processors.

Canada:

1. Reach Security takes steps to ensure that Reach Security's Sub-processors, as described in Section 3 (Sub-processing) of the DPA, are third parties under PIPEDA, with whom Reach Security has entered into a written contract that includes terms substantially similar to this DPA. Reach Security conducts appropriate due diligence on its Sub-processors.
2. Reach Security will implement technical and organizational measures as set forth in Section 4 (Security) of the DPA.