Directly Data Protection Addendum (“DPA”)

This Data Protection Addendum (“**DPA**") is incorporated into the Master Services Agreement or “**MSA**” (“**Agreement**”) between the parties identified in the applicable Directly Order Form for the provision of the Directly Platform and related services (collectively, the “**Services**”). If there is any conflict between this DPA and the Agreement regarding the parties’ respective privacy and security obligations, the provisions of this DPA shall control.

“DIRECTLY”: Directly, Inc.	**“CUSTOMER”:** [Customer Legal Name]
Signature:	**Signature:**
Printed Name:	**Printed Name:**
Title:	**Title:**
Data Protection Officer or Representative: David Phillips, General Counsel, dphillips@directly.com	**Data Protection Officer or Representative:**
Date:	**Date:**
Notices to Directly: Directly, Inc. Attn: Legal 333 Bryant Street, Suite 250 San Francisco, CA 94107 USA **With an email copy to:** legal@directly.com	**Notices to Customer:** **With an email copy to:** [Customer Email]

1. **General**

   a. **Purpose.** Applicable data protection laws, including but not limited to the European Union General Data Protection Regulation ("**GDPR**") and California Consumer Privacy Act ("**CCPA**," collectively "**DP Laws**"), require an agreement between entities sharing personal data or personal information. Processing, *inter alia*, must be conducted in accordance with technical and organizational measures that meet the requirements of the DP Laws and ensure the protection of the rights of data subjects, natural persons, consumers or households (as the case may be). This DPA is intended to satisfy these requirements for the parties. For the avoidance of doubt, each party is only responsible for the local, state, national and/or foreign law, treaties and/or regulations applicable to such party.

   b. **Applicability.** This DPA applies exclusively to the processing of Customer Data that is subject to DP Laws in the scope of the Agreement between the parties for the provision of Services. The DPA does not limit or reduce any data protection commitments Processor makes to Controller in any other agreement between Processor and Controller.

   c. **Effective Date.** Processor makes the commitments in the DPA effective on the date Processor begins to process Personal Data on behalf of a Controller.

2. **Defined Terms.** The terms of the Agreement are incorporated into this DPA. Any capitalized term not defined in this DPA will have the meaning ascribed to that term in the Agreement. Terms used but not defined in the Agreement or DPA will have the same meaning as set forth in the GDPR or the CCPA as context or applicable law requires. Without limiting the generality of the foregoing, the following terms are used in this DPA:

   a. "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data. Unless otherwise specified, Customer is the controller of Customer Data, Personal Data and Personal Information under the Agreement.

   b. "**Customer Data**" means any data, including but not limited to Personal Data or Personal Information that Customer or Customer's authorized users input, upload to the Service or otherwise provide to Directly, which it processes in the context of providing Services.

   c. "**Data Subject**" means the individual to whom Personal Data relates.

   d. "**Personal Data**" or "**Personal Information**" are used contextually to mean any data or information relating to an identified or identifiable natural person that has been provided by a Customer for processing through the Services and includes personal information that can identify, relate to, describe, be associated with, or be reasonably capable of being associated with a particular consumer or household.

   e. "**Process(ing)**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

   f. "**Processor**" means an entity which engages in the Processing of Personal Data on behalf of the Controller. Unless otherwise specified, Directly is the processor of Customer Data, Personal Data and Personal Information under the Agreement.

   g. "**Service(s)**" means any service or services to be performed by the Processor under the Agreement.

   h. "**Standard Contractual Clauses**" means the model clauses for the transfer of personal data to processors established in third countries approved by the European Commission, the approved version of which is set out in the European Commission's Decision 2010/87/EU of 5 February 2010.

i. As used in this DPA, the terms “**Business**”, “**Commercial Purpose**”, “**Consumer**”, “**Personal Information**”, “**Service Provider**”, “**Sell**” and “**Verifiable Consumer Request**” have the meanings given in the CCPA.

3. **Roles & Instructions.** Unless indicated otherwise, Directly will act as and be referred to as the “**Processor**” and the Customer will act as and be referred to as a “**Controller**” with respect to any personal data or personal information. The Agreement and the DPA (including terms and conditions incorporated by reference in either the Agreement or the DPA) are Customer’s current instructions to Processor for the processing of Personal Data, but may be modified in writing to align with any requirements of the DP Laws, industry standards or by the instructions of any party who serves as a Controller under the DP Laws. A description of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 1.

4. **Data Processing Description.** Annex 1 to this DPA describes the data exporter, data importer, data subjects, data categories, special data categories (if appropriate), the processing operations and the technical and organizational measures implemented by Subprocessor to protect the Personal Data. The Agreement describes the subject matter of the processing of Personal Data, the duration of data processing, the nature and purpose of the processing and the obligation and rights of the Processor.

5. **Customer Instructions.** Customer appoints Directly as a processor to process Customer Data on behalf of, and in accordance with, Customer’s instructions as set out in the Agreement and this DPA, as otherwise necessary to provide the Services, or as otherwise agreed in writing. Customer shall ensure that its instructions comply with all laws, regulations and rules applicable to the Customer Data, and that Directly’s processing of the Customer Data in accordance with Customer’s instructions will not cause Directly to violate DP Laws. Directly agrees not to use Customer Data, except as necessary to maintain or provide the Services, or as necessary to comply with the law or other binding governmental order.

6. **Contractual Terms.** This Section reproduces, with edits for clarity, the relevant contractual terms required by the GDPR and the CCPA.

   a. The Processor shall not engage another processor without general written authorization of the Processor. In the case of general written authorization, Processor shall inform Controller of the initial set of processors and any intended changes concerning the addition or replacement of other processors, thereby giving Controller the opportunity to object to such changes. In particular, Processor shall:

      i. process the Personal Data only on documented instructions from Processor, including with regard to transfers of Personal Data to a third country or an international organization unless required to do so by a government body or law to which Processor is subject; in such a case, Processor shall inform Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

      ii. ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

iii. take all measures required pursuant to Article 32 of the GDPR.

iv. respect the conditions referred to herein for engaging another processor.

v. taking into account the nature of the processing, assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights under DP Laws.

vi. assist Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Subprocessor.

vii. at the choice of Controller, delete or return all the Personal Data to Processor after the end of the provision of Services relating to processing and delete existing copies unless Applicable DP Laws require storage of the Personal Data.

viii. make available to Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller, and immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other European Union or Member State data protection provisions.

b. Where Processor engages another processor or sub-processor for carrying out specific processing activities on behalf of Processor, the same data protection obligations as set out in this DPA shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the DP Laws. Where that other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other subprocessor's obligations.

c. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Controller and Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (A) the pseudonymisation and encryption of Personal Data; (B) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services; (C) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (D) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

d. In assessing the appropriate level of security, consideration shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

e. Controller and Processor shall take steps to ensure that any natural person acting under the authority of Processor or Subprocessor who has access to Personal Data does not process them except on instructions from Processor, unless he or she is required to do so by

European Union or Member State law.

f. Processor shall notify Controller without undue delay after becoming aware of a personal data breach. Such notice will, at a minimum, (A) describe the nature of the Personal Data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (B) communicate the name and contact details of the data protection officer, representative or other contact where more information can be obtained; (C) describe the likely consequences of the personal data breach; and (D) describe the measures taken or proposed to be taken to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

g. Processor provides Services to Customer pursuant to an Agreement between the parties, and the parties wish to clarify their roles and relationship with regard to the CCPA. To the extent the CCPA applies to either party, then this DPA pertains to data constituting Personal Information under the CCPA.

h. Customer collects the Personal Information included in the data and determines the means and purposes of its processing, and therefore is a Business; Directly processes the data for a business purpose on behalf of Customer, and is therefore a Service Provider.

i. Customer's transfer of data to Directly is not a Sale, and Directly provides no monetary or other valuable consideration to Customer in exchange for the data.

j. Except as otherwise instructed by Customer, Directly will not (a) sell the Personal Information or (b) collect, retain, use or disclose Personal Information for any purpose (including any Commercial Purpose) other than to provide the Services as provided in the Agreement.

k. Directly certifies that it understands its contractual obligations under the Agreement and shall comply with such contractual obligations.

l. As applicable to the Service, and taking into account Directly's access to the data, Directly will reasonably assist Customer with any verifiable consumer request to exercise rights under DP Laws.

7. **Responding to Third Party Requests.** In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory or third party is made to Directly in connection with the processing of Customer Data, Directly shall direct the inquirer to the Customer's relevant web page and/or inform Customer providing details of the same, to the extent legally permitted. Unless legally obligated to do so, Directly shall not respond to any such request, inquiry or complaint without Customer's prior consent except to confirm that the request relates to the customer or end user to which Customer hereby agrees.

8. **Confidentiality Obligations of Directly Personnel.** Directly will ensure that any person it authorizes to process the Customer Data shall protect the Customer Data in accordance with confidentiality obligations under the Agreement.

9. **Subcontracting.** Customer consents to Directly engaging third party sub-processors to process Customer Data under this DPA provided that:

   a. A current list of sub-processors, including the identity of each of those sub-processors and its country location, has been provided to Customer or is available at: https://www.directly.com/legal/subprocessors ("**Sub-processor List**"). Directly will either send Customer an email to the address set above, or provided, informing Customer of any new sub-processors or Directly will enable Customer to receive notifications of new sub-processors by emailing subprocessor@directly.com with the subject "Subscribe." If Customer objects to a new sub-processor (which objection must be reasonable, based on specific written details, and made, if at all, within thirty (30) days after Directly has first included the proposed new sub-processor), the parties will work in good faith to resolve the objection in accordance with the subsection below.

   b. Customer may object to Directly's appointment or replacement of a sub-processor within ten (10) days of Directly informing Customer of such appointment or replacement (as described below, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, the parties shall discuss commercial reasonably alternative solutions in good faith. If the parties do not reach resolution within ten (10) days of Customer's objection, and Directly does not remove the new or replacement sub-processor, Customer may suspend or terminate the Agreement. Directly imposes data protection terms on any sub-processor it appoints that require it to protect the Customer Data to the standard required by DP Laws. Directly remains liable for any breach of this DPA that is caused by an act, error or omission of its sub-processor.

10. **Data Subject Right Requests.** Directly can provide company customers with API self-service features, where a participating customer can submit requests to delete user data. To assist in the implementation of these automated features, please refer to our API documentation here: https://developer.directly.com/messaging-api.html. In addition, Directly will provide reasonable assistance (at Customer's expense) to the extent the self-service features of the Services do not sufficiently enable Customer to comply with its obligations with respect to data subject rights under DP Laws. For example, if Customer needs to submit such a request while Customer implements that API, Customer can send any delete requests to Directly at subject_requests@directly.com, Directly will log a request through our JIRA system for the Directly engineering team to execute the deletion request.

11. **Return or Deletion of Customer Data.** Following termination or expiration of the Agreement, Directly will provide a reasonable opportunity for Customer to obtain a copy of its Customer Data or delete the same upon written request. This requirement shall not apply to the extent that Directly is required or permitted by law to retain some or all of the Customer Data, or to Customer Data it has archived on backup systems, which Directly shall securely isolate and protect from any further processing except to the extent required by law.

12. **Directly Audit Program.** The parties acknowledge that Customer must be able to assess Directly's compliance with its obligations under DP Laws insofar as Directly is acting as a processor on behalf of Customer. For the purpose of verifying Directly's compliance with DP Laws and the Agreement and upon reasonable notice of no less than thirty (30) days, Directly agrees to permit Customer, at Customer's cost and no more than once annually, to conduct

audits through a Directly approved third party auditor. However, Directly agrees to allow audits to be conducted directly by Customer where, under DP Laws, (a) Customer has the right to conduct audits directly; and (b) such right cannot be contractually waived by Customer. Directly agrees to cooperate in good faith with the audit and promptly (i) provide access to books, records (including, but not limited to, security scan records), and other information necessary for the audit, and (ii) at Customer's request enable access to Directly's premises if absolutely necessary to properly conduct the audit or required under DP Laws. Customer agrees to schedule audits to minimize disruption to Directly's business, require any third party it employs to sign a non-disclosure agreement, and make the results of the audit available to Directly. Customer will only disclose the results of the audit to third parties if such disclosure is required to demonstrate Customer's own compliance, or otherwise required under applicable laws.

13. **Violations of Applicable Data Protection Law.** Directly will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate DP Laws.

14. **Transparency.** The parties acknowledge that Directly does not have a direct relationship with Customer's end users whose personal data Directly may process in connection with Customer's use of the Services. Customer shall be responsible for ensuring its end users are provided adequate notice of Directly's processing activities. Directly will provide Customer with sufficient information regarding its processing activities to allow Customer to provide such notice.

15. **Security.**

   a. **Security Measures:** Directly has implemented and will maintain appropriate technical and organizational measures to protect Customer Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Security Incident**"). The measures Directly takes to protect Customer Data from a Security Incident include those described at https://www.Directly.com/legal/security.

   b. **Configuration of Directly Technology:** Customer is responsible for properly configuring and implementing the Services and using available features and functionalities to maintain appropriate security in light of the nature of the data processed by Customer's use of the Services.

   c. **Security Incident Notification - Customer Data:** Directly shall, to the extent permitted by law, promptly notify Customer of any Security Incident of which Directly becomes aware. To the extent such Security Incident is caused by a violation of the requirements of this DPA by Directly, Directly shall make reasonable efforts to identify and remediate the cause of such Security Incident. Directly shall provide reasonable assistance to Customer in the event that Customer is required under DP Laws to notify a supervisory authority or any data subjects of the Security Incident.

   d. **Security Incident Notification - Customer Account Data:** If Directly becomes aware of a confirmed Security Incident involving Customer Data containing the personal data of data subjects with whom Directly does not have a direct relationship, for example Customer's end users, and Directly determines that the incident must be reported to a regulatory authority, Directly will notify the Customer of the incident and of its obligation and intent to notify the regulatory authority. If the impacted data subjects are required to be notified of the Security Incident, Customer will provide reasonable assistance to Directly to effectuate appropriate notice to the impacted data subjects.

16. **International Transfers.**

a. Customer acknowledges that, as of the Effective Date of this DPA, Directly's primary processing facilities are in the United States. To the extent that Customer's use of the Services requires transfer of personal data out of the European Economic Area ("**EEA**"), Directly will take such measures as are necessary to ensure the transfer is in compliance with DP Laws. Such measures include (without limitation) transferring the Customer Data to a recipient that has executed an agreement with Standard Contractual Clauses adopted or approved by the European Commission. The Standard Contractual Clauses as set forth in Annex 3 to this Addendum.

b. **Standard Contractual Clauses:** The parties further agree that the Standard Contractual Clauses in Annex 3 to this DPA will apply to personal data within Customer Data that is transferred from the European Economic Area and/or Switzerland to outside the European Economic area and Switzerland, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive).

17. **Entire Agreement; Conflict.** This DPA supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this DPA, including any prior data processing addenda entered into between Directly and Customer. If there is any conflict between this Addendum and any agreement, including the Agreement, the terms of this DPA shall control.

ANNEX 1 - DETAILS OF THE PROCESSING

Description of Data Exporter - This Annex 1 forms part of the SCCs and must be completed and signed by the parties.

Data exporter - The “data exporter” is identified in the Order Form to which this Agreement is incorporated. Data Exporter provides (please briefly specify your activities relevant to the transfer):

The data exporter is (i) the legal entity that has executed the Agreement and/or these Standard Contractual Clauses as a data exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased SCC Services on the basis of one or more Order Form(s).

Data importer - The data importer is (please specify briefly activities relevant to the transfer):

Directly, Inc. Data importer’s services are the provision of a platform for customer support (“Services”) which after configuration by the data exporter processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects - The personal data transferred concern the following categories of data subjects (please specify):

- *The Data Subjects are customer users of Data Exporter Customer authorized by it to use the Services.*
- *Employees, agents, advisors, freelancers of Data Exporter (who are natural persons)*

Categories of data - The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, subject to the data exporter configuration of Directly’s technology, the following categories of Personal Data:

- *Customer User first and last name*
- *Customer User email address/and/or mobile number*
- *Customer User request information (e.g., text of request thread)*
- *Customer User ID data (ID number – internal/external)*
- *Customer User log data (e.g., IP address, browser type, mobile network information).*
- *Data about question type (question category and language type)*
- *Customer Employee contact information (company, email, phone, physical business address)*

Special categories of data (if appropriate) - The Personal Data transferred concern the following special categories of data (please specify):

None as of the Effective Date.

Processing operations - The Personal Data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement. Specific processing operations are described in Section 2 of the Addendum to which these Clauses are attached.

ANNEX 2 - TO MSA & THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

See Section 12 of the DPA to which these Clauses are attached.

ANNEX 3 - TO MSA & THE STANDARD CONTRACTUAL CLAUSES (Processors)

Available here: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087