DATA PROCESSING ADDENDUM
(Last Updated September 2, 2022)

This Data Processing Addendum, including its Exhibits and Appendices ("**DPA**") forms part of the Service Subscription Agreement (the "**Agreement**") between Enlyft, Inc. ("**Enlyft)** and the Subscriber that is a Party the Agreement. Enlyft and Subscriber may each be referred to herein as "**Party**" or collectively as "**Parties**." Capitalized terms not defined herein have the same meaning set forth in the Agreement. In the course of providing the Services under the Agreement, Enlyft may Process Personal Data on Subscriber's behalf and the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data. By executing the Agreement, Subscriber enters into this DPA on behalf of Subscriber and Subscriber's Authorized Affiliates. For the avoidance of doubt, Subscriber's signature of the DPA on Page 9 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses and all other schedules and exhibits attached hereto.

1. DATA PROCESSING TERMS.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition, means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Subscriber's Affiliate(s) which (a) is subject to Data Protection Laws and (b) is permitted to use the Services pursuant to the Agreement between Subscriber and Enlyft but has not signed its own Agreement with Enlyft and is not "Subscriber" as defined under the Agreement.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code§ 1798.100 et seq., and its implementing regulations.

"**Controller**" means the entity which determines the means and purposes of the Processing of Personal Data.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including without limitation CCPA and other laws and regulations of the United States and its states, the GDPR and other European Data Protection Laws, each as amended from time to time.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**Europe**" means the European Union, the European Economic Area, Switzerland, and the United Kingdom.

"**European Data Protection Laws**" means the GDPR and other laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, each as amended from time to time.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) together with any subordinate legislation or implementing regulation.

"**Personal Data**" or **"Personal Information"** means Subscriber Data that is information describing or relating to an identified or identifiable natural person or household or an identified or identifiable legal entity and where such information is protected as personal data or personally identifiable information under applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"**Processor**" means the Party that Processes Personal Data on behalf of the Controller, including as applicable any "Service Provider" as that term is defined by the CCPA.

"**Standard Contractual Clauses**" or "**SCCs**" means 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 approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"**Sub-processor**" means any Processor engaged by Enlyft to perform services under the Agreement on behalf of Enlyft.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

"**Subscriber Data**" has the same meaning as defined in the Agreement, provided that such data is electronic data and information submitted by or for Subscriber to the Services.

2. PROCESSING OF PERSONAL DATA.

2.1. **Roles of the Parties**. The Parties acknowledge and agree that (i) with regard to the Processing of Personal Data, Subscriber is the Controller and Enlyft is the Processor and (ii) Enlyft will engage Sub-processors pursuant to the requirements set forth in Section 5 (Sub-Processors).

2.2. **Duration.** Enlyft shall process Personal Data throughout the duration of the term of the Agreement or any renewal term thereof. Upon termination of the Services by either Party, Enlyft shall cease processing Personal Data on Subscriber's behalf upon completion of the termination provisions described herein.

2.3. **Subscriber Processing of Personal Data**. Subscriber shall, in its use of the Services, Process Personal Data in accordance with the requirements of all applicable Data Protection Laws, including without limitation requirements to provide notice to Data Subjects of the use of Enlyft as Processor. Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Subscriber acquired Personal Data. Subscriber represents and warrants that Subscriber has established a lawful basis to Process Personal Data, Subscriber's use of the Services will not violate the rights of any Data Subject, and Subscriber has the right to transfer, or provide access to, the Personal Data to Enlyft for Processing

in accordance with the terms of the Agreement (including this DPA). Subscriber shall inform Enlyft without undue delay if Subscriber is unable to comply with its obligations under this DPA or any applicable Data Protection Laws. For the avoidance of doubt, Enlyft is not responsible for compliance with any Data Protection Laws applicable to Subscriber or Subscriber's industry that are not generally applicable to Enlyft.

2.4.   Enlyft's Processing of Personal Data. Subscriber hereby appoints Enlyft to process the Personal Data contained in Subscriber Data on behalf of Subscriber as necessary for Enlyft to provide the Services under the Agreement. All Personal Data Processed under the Agreement (including this DPA) will be stored, organized, and made available to Subscriber as the Controller. Enlyft shall treat Personal Data as Confidential Information. If Enlyft is required by applicable law to disclose Subscriber Data for a purpose unrelated to the Agreement, Enlyft will first inform Subscriber of the legal requirement and give Subscriber an opportunity to object or challenge the requirement, unless the law prohibits such notice. Notwithstanding the foregoing, Enlyft shall have the right to collect and use Personal Data contained in Subscriber Data to investigate a use of the Service that is unlawful or violates the Agreement, provide, and develop the Service, respond to legal actions, or for administrative purposes such as accounting and compliance.

2.5.   Nature, Purpose, and Subject-Matter of the Processing. The nature and purpose of Enlyft's Processing of Personal Data as Subscriber's Processor is described in and governed by the Agreement. The subject-matter of data Processed under this DPA is Personal Data of Subscriber's employees, contractors, representatives, and other end user Data Subjects and as otherwise described in the Agreement. Enlyft shall only Process Subscriber Data for the purpose of providing the Services to Subscriber and to comply with Subscriber's Instructions. For each Service for which Processing is involved, the duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 hereto (**Description of Processing/Transfer**).

2.6.   Instructions. Enlyft shall Process, retain, use, store, or disclose Personal Data only according to written, documented instructions issued by Subscriber to Enlyft to perform a specific or general action with regard to Personal Data for the purpose of providing the Services to Subscriber pursuant to the Agreement ("**Instructions**"). The Parties agree that the Agreement (including this DPA), together with Subscriber's use of the Services in accordance with the Agreement, constitute Subscriber's complete and final Instructions to Enlyft in relation to the Processing of Subscriber Data. Subscriber may modify, amend, add, or replace individual Instructions in writing ("**Additional Instructions**") by email to Subscriber's designated Enlyft contact. Any Additional Instructions must be consistent with this DPA and the Agreement. If Enlyft determines that Additional Instructions are outside the scope of the Agreement, Enlyft may charge additional fees and/or require a written agreement between Enlyft and Subscriber to perform such Additional Instructions. Enlyft shall inform Subscriber without delay if, in Enlyft's opinion, an Instruction violates applicable Data Protection Laws or Enlyft is unable follow an Instruction and, where necessary, cease all Processing until Subscriber issues new Instructions with which Enlyft is able to comply.

3.   RIGHTS OF DATA SUBJECTS

Enlyft shall, to the extent legally permitted, promptly notify Subscriber if Enlyft receives a request from a Data Subject to exercise the Data Subject's right under applicable Data Protection Laws relating to Subscriber Data, each such request being a "**Data Subject Request.**" Taking into account the nature of the Processing, if Subscriber is unable to independently address a Data Subject Request, Enlyft will assist Subscriber by appropriate technical and organizational measures, insofar as this is possible and to the extent Enlyft is legally permitted to do so, for the fulfilment of Subscriber's obligation to respond to a Data Subject Request under Data Protection Laws. Subscriber shall be legally responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data and for all costs associated with the same.

4.   ENLYFT PERSONNEL

4.1.   Confidentiality. Enlyft shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Enlyft shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2.   Reliability. Enlyft shall take commercially reasonable steps to ensure the reliability of any Enlyft personnel engaged in the processing of Personal Data.

4.3.   Limitation of Access. Enlyft shall ensure that Enlyft's access to Personal Data is limited to those personnel who are necessary to provide the Services.

4.4.   Data Protection Officer. Enlyft has appointed a data protection officer. The appointed person may be reached at privacy@enlyft.com.

5.   SUB-PROCESSORS

5.1.   Appointment of Sub-processors. Subscriber authorizes Enlyft to engage the Sub-Processors on our Sub-Processor List as of the Effective Date to Process Subscriber Data pursuant to the Agreement (including this DPA) and Subscriber acknowledges and agrees that (i) Enlyft's Affiliates may be retained as Sub-processors and (ii) Enlyft may engage third-Party Sub-processors in connection with the provision of the Services. Enlyft or a Enlyft Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Subscriber Data to the extent applicable to the nature of the services provided by such Sub-processor. Enlyft shall be liable for the acts and omissions of its Sub-processors to the same extent Enlyft would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.2.   Sub-processor List, Notification, and Objection. Upon written request, Enlyft shall make available to Subscriber a current list of Sub-processors for the Services. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location. Enlyft shall give Subscriber at least thirty (30) days' prior written notice if Enlyft engages a new Sub-processor that will process Personal Data pursuant to the Agreement. Subscriber may object to Enlyft's use of a new Sub-processor by notifying Enlyft promptly in writing within ten (10) business days after receipt

of such notice. In the event Subscriber objects to a new Sub-processor, as permitted in the preceding sentence, Enlyft will use reasonable efforts to make available to Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Subscriber. If Enlyft is unable to make available such change within thirty (30) days of the objection notice, Subscriber may terminate the Agreement with respect only to those Services which cannot be provided by Enlyft without the use of the objected-to new Sub-processor by providing written notice to Enlyft. Enlyft will refund Subscriber any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Subscriber.

6. SECURITY

6.1. Security Controls. Enlyft shall maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of Subscriber Data. In doing so, Enlyft shall take 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. Subscriber is solely responsible for (i) determining whether the Services meet Subscriber's security standards and support Subscriber's obligations under Data Protection Laws and (ii) the secure use of Enlyft's Services by Subscriber or any individual Subscriber provide with a device listed on or access to Subscriber's account ("**User**") , including but not limited to securing account authentication information and ensuring no User seeks to misuse Personal Data or engages in activities likely to give rise to a Data Incident (defined in Section 7) impacting Subscriber Data.

6.2. Demonstration of Compliance. Upon Subscriber's written request and with at least thirty (30) days' notice (or a shorter period if required by applicable law), Enlyft shall make available to Subscriber (on a confidential basis) all information reasonably necessary and allow for and contribute to Subscriber's audits to demonstrate Enlyft's compliance with this DPA ("**Audits**"), provided that Subscriber shall not exercise this right more than once per year. In response to a request for such information related to an Audit, Enlyft shall provide to Subscriber: (i) if available, a copy of Enlyft's most recent third-party audits or certifications relating to the topic of such request or (ii) copies of Enlyft's records or documents that Enlyft determines to be relevant and appropriate to the request. Subscriber has no right to access: (a) records or documents not directly related to Enlyft's Processing of Personal Data under this DPA or (b) any part of Enlyft's information system, data hosting sites or centers, or infrastructure. Subscriber must conduct all Audits (x) during normal business hours; (y) according to security and confidentiality terms and guidelines; and (z) taking reasonable measures necessary to prevent unnecessary disruption to Enlyft's operations. Subscriber shall be responsible for all costs and expenses arising from such audit, including the reasonable costs and expenses of Enlyft in complying with an Audit request. The information disclosed hereunder and the results of an Audit shall be considered Confidential Information. Subscriber acknowledges that certain Sub-processors to Enlyft may require Subscriber to execute a non-disclosure agreement with them before the Sub-processor will produce the requested information related to an Audit.

6.3. Data Protection Impact Assessment. Upon Subscriber's request, Enlyft shall provide Subscriber with reasonable cooperation and assistance needed to fulfil Subscriber's obligation under Data Protection Laws to carry out a data protection impact assessment related to Subscriber's use of the Services, to the extent Subscriber does not otherwise have access to the relevant information and to the extent such information is available to Enlyft.

7. DATA INCIDENT MANAGEMENT; NOTIFICATION

Enlyft shall notify Subscriber without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Subscriber Data, including Personal Data, transmitted, stored or otherwise (a "**Data Incident**") Processed by Enlyft or its Sub-processors occurring on Enlyft or our Sub-Processor's information system of which Enlyft becomes aware. Enlyft shall make reasonable efforts to identify the cause of such Data Incident and take such steps as Enlyft deems necessary and reasonable to remediate the cause of such a Data Incident to the extent the remediation is within Enlyft's reasonable control. At Subscriber's reasonable request, and to the extent Enlyft is required to do so under applicable Data Protection Laws, Enlyft will promptly provide Subscriber with commercially reasonable assistance as necessary to enable Subscriber to meet Subscriber's obligations under applicable Data Protection Laws to notify authorities and/or affected Data Subjects. The obligations herein shall not apply to incidents that are caused by Subscriber or its Users.

8. GOVERNMENT ACCESS REQUESTS

If Enlyft receives a legally binding request from a government agency, state body, court, or other public authority ("**Public Authority**") to access Personal Data that Enlyft Processes on Subscriber's behalf ("**Government Access Request**"), Enlyft shall, unless otherwise legally prohibited, promptly notify Subscriber including a summary of the nature of the request. To the extent Enlyft is prohibited by law from providing such notification, Enlyft shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Enlyft to communicate as much information as possible, as soon as possible. Further, Enlyft shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Enlyft shall pursue possibilities of appeal. When challenging a request, Enlyft shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Enlyft agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Enlyft shall promptly notify Subscriber if Enlyft becomes aware of any direct access by a Public Authority to Subscriber Data and provide information available to Enlyft in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Enlyft to pursue action or inaction that could result in civil or criminal penalty for Enlyft such as contempt of court. Enlyft shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses

9. RETURN OR DELETION OF PERSONAL DATA

Upon termination or expiration of the Agreement or any renewal term thereof, Enlyft will delete all Personal Data Processed under the Agreement that is in Enlyft's possession.

In the case of any Personal Data not so deleted, Enlyft will return, destroy, or render anonymous all such Personal Data in accordance with Subscriber's reasonable written Instructions submitted to Enlyft within 30 days of termination or expiration of the Agreement, subject to the limitations described in the Agreement. The requirements of this Section 9 do not apply to the extent that Enlyft is required by applicable law to retain some or all of Subscriber Data, or to Subscriber Data that is archived on back-up systems, which data Enlyft shall securely isolate and protect from any further Processing and delete in accordance with Enlyft's deletion practices.

10. AUTHORIZED AFFILIATES

10.1. **Contractual Relationship**. The Parties acknowledge and agree that, by executing the Agreement, Subscriber executes this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Enlyft and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a Party to the Agreement and is only a Party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Subscriber. As the contracting Party to the Agreement, Subscriber shall remain responsible for coordinating all communication with Enlyft under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.2. **Rights of Authorized Affiliates**. Where an Authorized Affiliate becomes a Party to the DPA with Enlyft, except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Enlyft directly by itself, solely Subscriber as the contracting Party to the Agreement shall (i) exercise any right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) exercise any such rights under this DPA in a combined manner for itself and all of its Authorized Affiliates together, not separately for each Authorized Affiliate individually.

11. LIMITATION OF LIABILITY

Except as specifically provided in the EU C-to-P Transfer Clauses, each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Enlyft, whether in contract, tort or under any other theory of liability, is subject to Section 8 (Limitations of Liability) of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Enlyft's and its Affiliates' total liability for all claims from Subscriber and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Subscriber and all of its Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Subscriber and/or any Authorized Affiliate that is a contractual Party to any such DPA.

12. EUROPEAN SPECIFIC PROVISIONS

12.1. **Definitions**. This Section 12 shall apply only to the extent Enlyft Processes Personal Data subject to European Data Protection Laws as Subscriber's Processor. For the purposes of this section 12 and Schedule 1, "EU C-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

12.2. **European Data Protection Laws**. Enlyft will Process Personal Data in accordance with the European Data Protection Laws requirements directly applicable to Enlyft's provision of its Services.

12.3. **Transfer mechanisms for data transfers**. If, in the provision of the Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of Europe, the transfer mechanism listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws of Europe:

- **The EU C-to-P Transfer Clauses**. Where Subscriber and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Enlyft is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in Section 2 of Schedule 1.

12.4. **Impact of local laws**. As of the Effective Date, Enlyft has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Enlyft from fulfilling its obligations under this DPA. If Enlyft reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("**Local Laws**") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Subscriber. In such a case, Enlyft shall use reasonable efforts to make available to Subscriber a change in the Services or recommend a commercially reasonable change to Subscriber's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Subscriber. If Enlyft is unable to make available such change promptly, Subscriber may terminate the Agreement and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Enlyft in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Subscriber shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

13. CALIFORNIA SPECIFIC PROVISIONS

13.1. **Definitions.** This Section 13 shall apply only to the extent Enlyft Processes Personal Data that is subject to the protection of the CCPA ("**California Personal Information**") on Subscriber's behalf. For the purposes of this Section 13 these terms shall be defined as follows:

- "**Business**", "**Service Provider**", "**Sell**", and "**Share**" shall have the meanings given to them in the CCPA.

- "**Controller**" is replaced with "**Business**" wherever those terms appear in Sections 2 through 11 and Sections 14 and 15 of this DPA.

- "**Processor**" is replaced with "**Service Provider**" wherever those terms appear in Sections 2 through 11 and Sections 14 and 15 of this DPA.

13.2. **Responsibilities.** The Parties agree that Enlyft will Process California Personal Information contained in Subscriber Data as Subscriber's Service Provider in accordance with the CCPA and strictly for the business purpose of performing the Service under the Agreement. Enlyft shall not (i) Sell California Personal Information contained in Subscriber Data; (ii) Share California Personal Information contained in Subscriber Data with third Parties for cross-contextual behavioral advertising purposes; (iii) retain, use, or disclose California Personal Information contained in Subscriber Data for a commercial purpose other than for such business purpose or as otherwise permitted by the CCPA; or (iv) retain, use, or disclose California Personal Information contained in Subscriber Data outside of the direct business relationship between Subscriber and Enlyft. Subscriber agrees that Subscriber is solely liable for Subscriber's compliance with the CCPA in Subscriber's use of Enlyft's Service.

13.3. **Certification.** Enlyft certifies that it understands and will comply with the restrictions of Section 13.2.

13.4. **No CCPA Sale.** The Parties agree that Subscriber does not sell California Personal Information to Enlyft because, as a Service Provider, Enlyft may only use California Personal Information contained in Subscriber Data for the purposes of providing the Services to Subscriber.

14. **LIST OF SCHEDULES**

Schedule 1: Transfer Mechanisms for European Data Transfers and Schedule 2: Description of Processing/Transfer are incorporated into this DPA by this reference.

15. **LEGAL EFFECT**

By executing the Agreement, the Parties' authorized signatories have duly executed this DPA.

Schedule 1
Transfer Mechanisms for European Data Transfers

1. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

For the purposes of the EU C-to-P Transfer Clauses, Subscriber is the data exporter and Enlyft is the data importer, and the Parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses for the transfer of Personal Data, any references to "Subscriber" in this Schedule, include such Authorized Affiliate. Where this Schedule 1 does not explicitly mention EU C-to-P Transfer Clauses it applies to them.

1.1. **Reference to the Standard Contractual Clauses**. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

1.2. **Docking clause**. The option under clause 7 shall not apply.

1.3. **Certification of Deletion**. The Parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Enlyft to Subscriber only upon Subscriber's written request.

1.4. **Instructions**. This DPA and the Agreement are Subscriber's complete and final documented instructions at the time of signature of the Agreement to Enlyft for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Subscriber to Process Personal Data are set out in Section 2.4 and 2.6 of this DPA and include onward transfers to a third Party located outside Europe for the purpose of the provision of the Services.

1.5. **Security of Processing**. For the purposes of clause 8.6(a), Subscriber is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in the Enlyft Privacy Policy and applicable Enlyft policies governing data security and protection and Subscriber agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Enlyft provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with Section 7 (Data Incident Management and Notification) of this DPA.

1.6. **Audits of the SCCs**. The Parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 6.2 of this DPA.

1.7. **General authorisation for use of Sub-processors**. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Enlyft has Subscriber's general authorisation to engage Sub-processors in accordance with Section 5 of this DPA. Enlyft shall make available to Subscriber the current list of Sub-processors in accordance with Section 5.2 of this DPA. Where Enlyft enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the Services, Subscriber grant Enlyft authority to provide a general authorisation on Controller's behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.

1.8. **Notification of New Sub-processors and Objection Right for new Sub-processors**. Pursuant to clause 9(a), Subscriber acknowledges and expressly agrees that Enlyft may engage new Sub-processors as described in Sections 5.2 and 5.3 of this DPA. Enlyft shall inform Subscriber of any changes to Sub-processors following the procedure provided for in Section 5.2 of this DPA.

1.9. **Complaints - Redress**. For the purposes of clause 11, and subject to Section 3 of this DPA, Enlyft shall inform data subjects on its website of a contact point authorised to handle complaints. Enlyft shall inform Subscriber if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Subscriber. Enlyft shall not otherwise have any obligation to handle the request (unless otherwise agreed with Subscriber). The option under clause 11 shall not apply.

1.10. **Liability**. Enlyft's liability under clause 12(b) shall be limited to actual and proven damage caused by Enlyft's Processing of Personal Data on Subscriber's behalf as a Processor where Enlyft has not complied with its obligations under the GDPR specifically directed to Processors, or where Enlyft has acted outside of or contrary to Subscriber's lawful Instructions, as specified in Article 82 GDPR.

1.11. **Supervision**. Clause 13 shall apply as follows:

1.11.1. Where Subscriber is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Subscriber with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

1.11.2. Where Subscriber is not established in an EU Member State, but fall within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and have appointed a representative pursuant to Article

27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

1.11.3. Where Subscriber is not established in an EU Member State, but fall within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The Data Protection Commission of Ireland, 21 Fitzwilliam Square South, Dublin, 2 D02 RD28, Ireland shall act as competent supervisory authority.

1.11.4. Where Subscriber is established in the United Kingdom or fall within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as competent supervisory authority.

1.11.5. Where Subscriber is established in Switzerland or fall within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws.

1.12. Notification of Government Access Requests. For the purposes of clause 15.1(a), Enlyft shall notify Subscriber only, and not the Data Subject(s), in case of government access requests. Subscriber shall be solely responsible for promptly notifying the Data Subject as necessary.

1.13. Governing Law. The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

1.14. Choice of forum and jurisdiction. The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the Parties agree that the courts of either (i) Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

1.15. Appendix. The Appendix shall be completed as follows:

- The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

1.16. Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses. In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws of Switzerland ("Swiss Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

1.17. Conflict. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

Schedule 2
Description of Processing/Transfer

1.   LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*
Name: Subscriber as identified in registration
Address: Subscriber's address listed in registration
Role: For the purposes of the SCCs, Subscriber is a Controller.
Activities relevant to the data transferred under these clauses: Provision of the Services pursuant to the Agreement (including the DPA).
Contact person's name, position, and contact details: Subscriber's designated point of contact listed at registration
Signature: By agreeing to the Agreement and the DPA, Subscriber agrees to this Schedule 2, effective as of the date of the Agreement.
Role: For the purposes of the EU C-to-P Transfer Clauses Subscriber and/or Subscriber's Authorized Affiliates are a Controller.

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*
Name: Enlyft, Inc.
Address: 5209 Lake Washington Blvd. NE, Suite 110, Kirkland, WA, 98033
Contact person's name, position, and contact details:
             Tim O'Neil, CFO
             tim@enlyft.com
Role: Processor

2.   CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

•   Subscriber may submit Personal Data to the Services, the extent of which is determined and controlled by Subscriber in Subscriber's sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

•   Subscriber's prospects, customers, and business partners (who are natural persons)
•   Employees or contact persons of Subscriber's prospects, customers, and business partners
•   Subscriber's employees, consultants, contractors, agents and/or third Parties with whom Subscriber conducts business (who are natural persons)
•   Subscriber's Users authorized by Subscriber to use the Services

3.   CATEGORIES OF PERSONAL DATA TRANSFERRED

•   Subscriber may submit Personal Data to the Services, the extent of which is determined and controlled by Subscriber in Subscriber's sole discretion, and which may include, but is not limited to the following categories of Personal Data:

•   Identifiers
•   Employment-related information
•   Commercial information
•   Internet or similar activity

4. SENSITIVE DATA TRANSFERRED

The Parties do not anticipate the transfer of sensitive data under the Agreement.

5. FREQUENCY OF THE TRANSFER

Data is transferred on a continuous basis depending on Subscriber's use of the Services.

6. NATURE OF THE PROCESSING

The nature of the Processing is the provision of the Services pursuant to the Agreement

7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

Enlyft will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the relevant Documentation, and as further instructed by Subscriber in Subscriber's use of the Services.

8. DURATION OF PROCESSING

Subject to Section 2.2 of the DPA, Enlyft will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

9. SUB-PROCESSOR TRANSFERS

Sub-processor(s) will Process Personal Data as necessary to provide the Services pursuant to the Agreement. Subject to Section 5 of this DPA, the Sub-processor(s) will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing. Identities of the Sub-processors used for the provision of the Services and their country of location are available upon request.

10. COMPETENT SUPERVISORY AUTHORITY

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland shall act as the competent supervisory authority.

- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as the competent supervisory authority.

- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws

11. TECHNICAL AND ORGANIZATIONAL MEASURES

- In addition to the administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, Enlyft also had implemented the following technical and organizational measures:

- Organizational management responsible for development, implementation, and maintenance of Enlyft's information security program.

- Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Enlyft systems, monitoring and maintaining compliance with Enlyft policies and procedures, and reporting the condition of its information security and compliance to senior internal management.

- Maintain policies to ensure that policies and measures are regularly reviewed and improved where necessary.

- Communication with Enlyft applications utilizes cryptographic protocols to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model that allows for security controls between each layer.

- Data security controls including logical segregation of data, restricted (e.g. role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.

- Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

- Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking access promptly when employment terminates or changes in job functions occur).

- Password controls and prohibiting users from sharing passwords.

- System audit, event logging, and related monitoring procedures to record user access and system activity for routine review.

- Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Enlyft possession.

- Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Enlyft technology and information assets.

- Incident / problem management procedures to enable Enlyft to investigate, respond to, mitigate, and notify of events related to Enlyft technology and information assets.

- Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses and other malicious code.

- Business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.