



Data Processing Addendum

This Data Processing Addendum (“**DPA**”) is incorporated into, and is subject to the terms and conditions of, the Subscription Terms and Conditions or other terms (the “**Agreement**”) between Customer and EvenUp Inc. (“**EvenUp**”) applicable to the Customer’s use of the Service. This DPA shall be effective for the term of the Agreement and applies only to the extent EvenUp Processes Customer Personal Data (as defined below) on behalf of Customer in the provision of the Service. “Customer Personal Data” as used herein does not include, and this DPA does not apply to, any Protected Health Information (“**PHI**”) as defined under the Health Insurance Portability and Accountability Act of 1996, as amended, which, where required or applicable, will instead be governed by a separate Business Associate Agreement (“**BAA**”) entered into by the Parties.

1. Definitions

1.1. In this DPA:

- a) “**Customer Personal Data**” means Personal Data provided to EvenUp by or on behalf of Customer and/or generated for Customer in connection with the Service.
- b) “**Data Protection Law**” means all laws that apply to the Processing of Customer Personal Data under the Agreement, including the California Consumer Privacy Act and any binding regulations promulgated thereunder and other laws and regulations of the United States and its states, as amended from time to time.
- c) “**Data Subject**” means the individual to whom Customer Personal Data relates.
- d) “**Personal Data**” has the meaning given to it in the Data Protection Law, and includes “Personal Data,” “personally identifiable information,” and equivalent terms as such terms may be defined by the Data Protection Law.
- e) “**Processing**” (including its cognate “**Process**”) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- f) “**Security Incident**” means a material breach of EvenUp’s security leading to the unauthorized or unlawful access by a third party, or confirmed accidental or unlawful destruction, loss or alteration, of Customer Personal Data in EvenUp’s possession, custody or control. “Security Incidents” will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. Customer’s Instructions

2.1. EvenUp will Process Customer Personal Data only in accordance with Customer’s instructions as described in Schedule 1 to this DPA. By entering into this DPA, Customer instructs EvenUp to Process Customer Personal Data to provide the Service and to perform its other obligations and exercise its rights under the Agreement, including, without limitation, to (a) carry out the Service or the business of which the Service is a part, (b) carry out any benefits, rights, and obligations relating



to the Service, (c) maintain records relating to the Service, and (d) comply with any legal or self-regulatory obligations relating to the Service.

3. Processing of Customer Personal Data

- 3.1. EvenUp serves as a service provider or processor, meaning that EvenUp Processes Customer Personal Data at the direction of and on behalf of Customer.
- 3.2. Each party will comply with the obligations applicable to it under the Data Protection Law with respect to the Processing of Customer Personal Data. Customer represents and warrants that it has the necessary rights, consents and permissions to use Customer Personal Data and to enable EvenUp to Process Customer Personal Data as intended by the Parties under the Agreement.
- 3.3. When EvenUp Processes Customer Personal Data, it will:
 - a) Except as permitted by applicable law, the Agreement or this DPA, not (a) “sell” or “share” (each as defined in the Data Protection Law) Customer Personal Data, (b) retain, use, or disclose Customer Personal Data for any purpose other than for the specific purpose of providing the Service, (c) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and EvenUp, and (d) combine Customer Personal Data with any Personal Data other than Customer Personal Data;
 - b) Require EvenUp’s personnel who access Customer Personal Data to commit to protect the confidentiality of Customer Personal Data;
 - c) Provide reasonable assistance necessary for Customer to comply with its obligations under the Data Protection Law;
 - d) Promptly notify Customer of any request made by a Data Subject in relation to Customer Personal Data. EvenUp will, at Customer’s written request, provide Customer with reasonable assistance necessary for the fulfillment of Customer’s obligation to respond to requests for the exercise of Data Subjects’ rights under the Data Protection Law. EvenUp shall not respond to such requests other than confirming with the Data Subject that the request relates to Customer and Customer Personal Data. Customer shall be solely responsible for responding to such requests;
 - e) Unless prohibited by law, inform Customer if EvenUp receives a request, complaint or other inquiry regarding the Processing of Customer Personal Data;
 - f) Inform Customer if it can no longer comply with its obligations under this DPA. Upon notice to EvenUp, Customer may take reasonable and appropriate steps to remediate EvenUp’s use of Customer Personal Data in violation of this DPA; and
 - g) Upon termination of the Agreement, as instructed by Customer, delete or return Customer Personal Data, except where continued retention of Customer Personal Data is in accordance with applicable law or EvenUp’s policies, in which case EvenUp shall retain such Customer Personal Data in accordance with this DPA.

4. Subprocessing

- 4.1. Customer agrees that EvenUp may use third-party suppliers, including Affiliates, to Process Customer Personal Data on its behalf for the provision of the Service (each a “Subprocessor”). Prior to engaging any new Subprocessor that will process Customer Personal Data, EvenUp will provide Customer notice and an opportunity to object, and Customer will have ten (10) business days from such notice to submit any objection in writing.



- 4.2. When engaging any Subprocessor, EvenUp will enter into a written contract with such Subprocessor containing data protection obligations consistent with those in this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the services provided by such Subprocessor.

5. Data Security

- 5.1. EvenUp will implement and maintain technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data, as further described in Schedule 2 to this DPA. EvenUp may update the security measures from time to time, provided the updated measures do not decrease the overall protection of Customer Personal Data.
- 5.2. Customer agrees that, without limitation of EvenUp's obligations under Section 5.1 of this DPA, Customer is solely responsible for its use of the Service, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Service; (c) securing Customer's systems and devices that EvenUp uses to provide the Service; and (d) backing up Customer Personal Data. Customer agrees that the Service and EvenUp's security commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under the Data Protection Law, and provide a level of security appropriate to the risk in respect of Customer Personal Data.

6. Security Incidents

- 6.1. If EvenUp becomes aware of a Security Incident, EvenUp will: (a) notify Customer of the Security Incident without undue delay and in any event within seventy-two (72) hours after becoming aware of it; and (b) take reasonable steps to identify the cause of such Security Incident, minimize harm and prevent a recurrence.
- 6.2. Customer is solely responsible for complying with incident notification requirements applicable to Customer. EvenUp's notification of or response to a Security Incident under this Section will not be construed as an acknowledgement by EvenUp of any fault or liability with respect to the Security Incident.

7. Audit

- 7.1. EvenUp will make available to Customer, at Customer's request, reasonable information as necessary to demonstrate compliance with this DPA.
- 7.2. To the extent EvenUp makes available to Customer confidential summary reports (each, an "**Audit Report**") prepared by third-party security professionals, upon request from Customer, EvenUp may provide such Audit Report in satisfaction of any audit rights accorded to Customer pursuant to the Data Protection Law. The Audit Report shall be considered EvenUp's confidential information.
- 7.3. If Customer can demonstrate that it requires additional information, beyond the Audit Report, then Customer may request that EvenUp provide an audit, at Customer's cost, subject to reasonable confidentiality procedures. Such audit shall: (a) not include access to any information that could compromise confidential information relating to EvenUp's other customers or suppliers, EvenUp's technical and organizational measures, or any trade secrets; and (b) be performed upon not less



than thirty (30) days' notice, during regular business hours, and in such a manner as not to unreasonably interfere with EvenUp's normal business activities.

8. General

- 8.1. If there is any conflict between this DPA and the Agreement, this DPA will prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. In the event of a conflict between this DPA and any BAA executed between the Parties, the BAA will control to the extent of that conflict and with respect to the Processing of PHI.
- 8.2. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.
- 8.3. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party under this DPA is subject to the limitations of liability set out in the Agreement. Customer acknowledges that EvenUp is reliant on Customer for direction as to the extent to which EvenUp is entitled to Process Customer Personal Data on behalf of Customer in the provision of the Service. Consequently, EvenUp will not be liable under the Agreement for any claim brought by individuals to whom Customer Personal Data relates arising from (a) any action or omission by EvenUp in compliance with Customer's instructions, or (b) Customer's failure to comply with its obligations under the Data Protection Law.
- 8.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.



Schedule 1

Details of Processing

1. Categories of Data Subjects. This DPA applies to EvenUp's Processing of Customer Personal Data relating to Customer's authorized users, employees, contractors, and clients whose information appears in case records and documents Processed by EvenUp in the provision of the Service.
2. Types of Personal Data. The extent of Customer Personal Data Processed by EvenUp is determined and controlled by Customer in its sole discretion and includes names, email addresses, and other Personal Data that Customer may Process through the Service.
3. Types of Sensitive Personal Data. Customer Personal Data may include sensitive Personal Data incidentally contained in case materials uploaded by Customer, such as health-related information.
4. Subject-Matter and Nature of the Processing. Customer Personal Data will be subject to the Processing activities that EvenUp needs to perform in order to provide the Service pursuant to the Agreement.
5. Purpose of the Processing. EvenUp will Process Customer Personal Data for purposes of providing the Service as set out in the Agreement.
6. Duration of the Processing. Customer Personal Data will be Processed for the duration of the Agreement in accordance with the terms of this DPA.



Schedule 2

Technical Measures

EvenUp will implement and maintain the security practices and procedures set out below:

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of EvenUp's information security program.
2. Periodic review and assessment of risks to EvenUp's organization, monitoring and maintaining compliance with EvenUp's policies and procedures, and reporting the condition of its information security and compliance to internal senior management as appropriate.
3. Data security controls which include logical segregation of data, restricted (e.g., role-based) access and monitoring, and use of commercially available and industry standard encryption technologies for Customer Personal Data as appropriate.
4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.
5. Password controls designed to manage and control password strength and password management requirements for assigned EvenUp credentials as appropriate.
6. Change management procedures and tracking mechanisms designed to test, approve and monitor changes to EvenUp's technology and information assets.
7. Incident response procedures designed to allow EvenUp to investigate, respond to, mitigate and notify events related to EvenUp's technology and information assets.
8. Network security controls that provide for the use of enterprise firewalls 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, as appropriate.
9. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.