Data Processing Agreement

This Data Processing Addendum ("**DPA**") forms a part of the Customer Terms of Service found at https://www.TimeTap.com/terms.html/, unless Customer has entered into a superseding written master subscription agreement with Addy Systems, LLC d/b/a TimeTap ("TimeTap"), in which case, it forms a part of such written agreement (in either case, the "**Agreement**").

By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Controller Affiliates. Customer and Processor are hereinafter jointly referred to as the "Parties" and individually as the "Party". All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, TimeTap may Process certain Personal Data (such terms defined below) on behalf of Customer and where TimeTap Processes such Personal Data on behalf of Customer the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Annex 1.
2. This DPA has been pre-signed on behalf of TimeTap.
3. To complete this DPA, Customer must complete the information in the signature box and sign on Page 9.
4. Send the completed and signed DPA to TimeTap by email, indicating Customer's Login (email address) (as set out on the applicable Order Form), to info@timetap.com
   Upon receipt of the validly completed DPA by TimeTap at this email address, this DPA will become legally binding.

A. HOW THIS DPA APPLIES TO CUSTOMER AND ITS AFFILIATES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the TimeTap entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with TimeTap or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the TimeTap entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

1. **Definitions**. In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth opposite each one of them:

"**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 50% of the voting interests of the subject entity.

"**Applicable Laws**" means (a) European Union or Member State laws with respect to any Customer Personal Data in respect of which Customer is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Customer Personal Data in respect of which the Customer is subject to any other Data Protection Laws

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

"**Controller Affiliate**" means any of Customer's Affiliate(s) (a) (i) that are subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Services pursuant to the Agreement between Customer and TimeTap, but have not signed their own Order Form and are not a "Customer" as defined under the Agreement, (b) if and to the extent TimeTap processes Personal Data for which such Affiliate(s) qualify as the Controller.

"**Customer Personal Data**" means any Personal Data Processed by Processor on behalf of Customer pursuant to or in connection with the Agreement;

"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other applicable country as agreed in writing between the Parties, including in Israel;

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

"**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).

"**Restricted Transfer**" means (i) a transfer of Customer Personal Data from Customer to Processor; or (ii) an onward transfer of Customer Personal Data from a Processor to a Sub Processor, or between two establishments of Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

"**Sub Processor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to Process Personal Data on behalf of the Customer in connection with the Principal Agreement; and

The terms, "**Commission**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

2. **Customer's Processing of Personal Data**.

2.1 Customer shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

3. **TimeTap's processing of Personal Data**.

3.1. Processor shall not Process Customer's Personal Data other than on the Customer's documented reasonable and customary instructions as specified in the Agreement or this DPA, unless such Processing is required by Applicable Laws to which the Processor is subject.

3.2. Customer instructs Processor (and authorizes Processor to instruct each Sub Processor) to (i) Process Customer's Personal Data; and (ii) in particular, transfer Customer Personal Data to any country or territory, all as reasonably necessary for the provision of the Services and consistent with the Agreement (including the Privacy Policy, as defined under the Agreement) and in accordance with Applicable Laws.

3.3. Furthermore, Customer warrants and represents that it is and will remain duly and effectively authorized to give the instruction set out in Section "A" and any additional instructions as provided pursuant to the Agreement and/or in connection with the performance thereof, on behalf of itself and each relevant Controller Affiliate, at all relevant times and at least for as long as the Agreement is in effect and for any additional period during which Processor is lawfully processing the Customer Personal Data.

3.4. Customer sets forth the details of the Processing of Customer Personal Data, as required by article 28(3) of the GDPR in **Annex 1** (Details of Processing of Customer Personal Data), attached hereto.

4. **Processor Personnel**. Processor shall take reasonable steps to ensure that access to the Customer Personal Data is limited on a need to know/access basis, and that all Processor personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Customer's Personal Data.

5. **Security**. Processor shall, in relation to the Customer Personal Data, implement appropriate technical and organizational measures to ensure an appropriate level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR. In assessing the appropriate level of security, Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Sub Processing**.

6.1. Customer authorizes Processor and each Processor Affiliate to appoint (and permit each Sub Processor appointed in accordance with this Section 6 to appoint) Sub Processors in accordance with this Section 6 and any restrictions in the Agreement.

6.2. Processor and each Processor Affiliate may continue to use those Sub Processors already engaged by Processor or any Processor Affiliate as of the date of this DPA. It is acknowledged and agreed that as of the date of this DPA Processor uses Amazon Web Services and Akamai as Sub Processors for the purpose of cloud hosting services and content delivery network, which use is subject to the respective Amazon and Akamai applicable guidelines.

6.3. Processor may appoint new Sub Processors and shall give notice of the appointment of any new Sub Processor (for instance as part of a Privacy Policy amendment), whether by general or specific reference to such Sub Processor (e.g., by name or type of service), including relevant details of the Processing to be undertaken by the new Sub Processor. If, within seven (7) days of such notice, Customer notifies Processor in writing of any objections (on reasonable grounds) to the proposed appointment, Processor shall not appoint for the processing of Customer Personal Data the proposed Sub Processor until reasonable steps have been taken to address the objections raised by Customer, and Customer has been provided with a reasonable written explanation of the steps taken. Where such steps are not sufficient to relieve Customer's reasonable objections then Customer or Processor may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub Processor without bearing liability for such termination. With respect to each new Sub Processor, Processor shall:

6.4.1. before the Sub Processor first Processes Customer Personal Data, take reasonable steps (for instance by way of reviewing privacy policies as appropriate) to ensure that the Sub Processor is committed to provide the level of protection for Customer Personal Data required by the Agreement; and

6.4.2. ensure that the arrangement between the Processor and the Sub Processor is governed by a written contract, including terms which offer materially similar level of protection for Customer Personal Data as those set out in this DPA that meet the requirements of Applicable Laws.

7. **Data Subject Rights**.

7.1. Customer shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g., for access, rectification, deletion of Customer Personal Data, etc.). Taking into account the

nature of the Processing, Processor shall reasonably endeavour to assist Customer insofar as feasible, to fulfil Customer's said obligations with respect to such Data Subject requests, as applicable, at Customer’s sole expense.

7.2. Processor shall:

6.2.1. promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2. ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by Applicable Laws, inform Customer of that legal requirement before it responds to the request.

8. **Personal Data Breach**.

8.1. Processor shall notify Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, in connection with the Processing of such Customer Personal Data by the Processor or Processor Affiliates. In such event, Processor shall provide Customer with information (to the extent in Processor’s possession) to assist Customer to meet any obligations to inform Data Subjects or Data Protection authorities of the Personal Data Breach under the Data Protection Laws.

8.2. At the written request of the Customer, Processor shall reasonably cooperate with Customer and take such commercially reasonable steps as are agreed by the parties or necessary under Privacy Protection Laws to assist in the investigation, mitigation and remediation of each such Personal Data Breach, at Customer’s sole expense.

9. **Data Protection Impact Assessment and Prior Consultation**.

9.1. At the written request of the Customer, the Processor and each Processor Affiliate shall provide reasonable assistance to Customer, at Customer's expense, with any data protection impact assessments or prior consultations with Supervising Authorities or other competent data privacy authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to Processing of Customer Personal Data by the Processor.

10. **Deletion or return of Customer Personal Data**.

10.1. Subject to Section 9.2, Processor shall promptly and in any event within up to sixty (60) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "Cessation Date"), delete or pseudonymize all copies of those Customer Personal Data, except such copies as authorized including under this DPA or required to be retained in accordance with applicable law and/or regulation.

10.2. Subject to the Agreement, Processor may retain Customer Personal Data to the extent authorized or required by Applicable Laws, provided that Processor shall ensure the

confidentiality of all such Customer Personal Data and shall ensure that it is only processed for such legal purpose(s).

10.3. Upon Customer's prior written request, Processor shall provide written certification to Customer that it has complied with this Section 10.

11. **Audit Rights**.

11.1. Subject to Sections 10.2 and 10.3, Processor shall make available to a reputable auditor mandated by Customer in coordination with Processor, upon prior written request, such information necessary to reasonably demonstrate compliance with this DPA, and shall allow for audits, including inspections, by such reputable auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Processor, provided that such third-party auditor shall be subject to confidentiality obligations.

11.2. Provisions of information and audits are and shall be at Customer's sole expense, and may only arise under Section 11.1 to the extent that the Agreement does not otherwise give Customer information and audit rights meeting the relevant requirements of the applicable Data Protection Laws. In any event, all audits or inspections shall be subject to the terms of the Agreement, and to Processor's obligations to third parties, including with respect to confidentiality.

11.3. Customer shall give Processor reasonable prior written notice of any audit or inspection to be conducted under Section 11.1 and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Processor's business. Customer and Processor shall mutually agree upon the scope, timing and duration of the audit or inspection in addition to the reimbursement rate for which Customer shall be responsible. Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1. to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2. if Processor was not given a written notice of such audit or inspection at least 2 weeks in advance;

11.3.3. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer has given notice to Processor that this is the case before attendance outside those hours begins; or

11.3.4. for premises outside the Processor's control (such as data storage farms of AWS or Akamai)

11.3.5. for the purposes of more than one (1) audit or inspection, in respect of each Processor, in any calendar year, except for any additional audits or inspections which:

11.3.5.1. Customer reasonably considers necessary because of genuine concerns as to Processor's compliance with this DPA; or

11.3.5.2. Customer is required to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Customer has identified its concerns or the relevant requirement or request in its prior written notice to Processor of the audit or inspection.

11.4 Customer shall reimburse TimeTap for any time expended for any such on-site audit at the TimeTap's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and TimeTap shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by TimeTap. Customer shall promptly notify TimeTap with information regarding any noncompliance discovered during the course of an audit, and TimeTap shall use commercially reasonable efforts to address any confirmed non-compliance.

12. **General Terms**

12.1. **Governing Law and Jurisdiction**.

12.1.1. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

12.2. **Order of Precedence**. Nothing in this DPA reduces Processor's obligations under the Agreement in relation to the protection of Personal Data or permits Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Privacy Policy (as defined under the Agreement), the Privacy Policy shall prevail provided only that the procedure prevailing through the Privacy Policy shall not constitute as a breach or infringement of any Applicable Laws. This DPA is not intended to, and does not in any way limit or derogate from Customer's own obligations and liabilities towards the Processor under the Agreement, and/or pursuant to the GDPR or any law applicable to Customer, in connection with the collection, handling and use of Personal Data by Customer or its Affiliates or other processors or their sub-processors, including with respect to the transfer or provision or Personal Data to Processor and/or providing access thereto to Processor. Subject to this Section 11.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in

writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

12.3. **Changes in Data Protection Laws**.

12.3.1. Customer may by at least forty-five (45) calendar days' prior written notice to Processor, request in writing any variations to this DPA if they are required, as a result of any change in, or decision of a competent authority under any applicable Data Protection Law, to allow Processing of those Customer Personal Data to be made (or continue to be made) without breach of that Data Protection Law; and

12.3.2. If Customer gives notice with respect to its request to modify this DPA under Section 12.3.1:

12.3.2.1. Processor shall make commercially reasonable efforts to accommodate such modification request, ; and

12.3.2.2. Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor for any further steps and costs associated with the variations made herein.

12.4. If Customer gives notice under Section 12.3.1, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days, then Customer or Processor may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof).

12.5. **Severance**. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the later date set out below.

Customer: [_____]

Signature: _____

Name: _____

Title: _____

Date: _____

Processor: TimeTap, Inc

Signature: Aditya Kapur

Name: _Aditya Kapur_____

Title: ____CEO_____

Date: ___April 7, 2020_____

Annex 1: Details Of Processing Of Customer Personal Data

This **Annex 1** includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data. The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement, including the Privacy Policy as references therein and this DPA.

The nature and purpose of the Processing of Customer Personal Data: rendering Services in the nature of a calendar management platform, as detailed in the Agreement and the Privacy Policy.

The types of Customer Personal Data to be Processed are as follows: As detailed in the Privacy Policy.

The categories of Data Subject to whom the Customer Personal Data relates to are as follows:
Customer's personnel and natural persons Data Subjects who are end users of the Customer's web and/or mobile application services.

The obligations and rights of Customer. The obligations and rights of Customer and Controller Affiliates are set out in the Agreement and this DPA.