



# Plannuh, Inc., Data Processing Agreement (DPA)

Updated November 2020

This Data Processing Agreement (“Agreement”) is made upon acceptance of the Main Agreement as defined below, between the customer entity accepting the terms of the Main Agreement (“Company”); and the Processor entering into the Main Agreement (“Plannuh”),

each a “Party” and together the “Parties”.

## RECITALS

- A. Plannuh and Company have entered into one or more agreements under which Plannuh supplies certain Subscription Services to Company from time to time as detailed in the various agreements (referred to collectively as the “Main Agreement”).
- B. The Parties have agreed that in order for Plannuh to perform its obligations pursuant to such Main Agreement, it will be necessary for Plannuh to Process certain Personal Data in respect of which Company will be a Data Controller, or acting on behalf of the Data Controller, for the purposes of this Agreement under and subject to the applicable Data Protection Laws (as defined below).
- C. The Parties have agreed to enter into this Agreement in order to address the compliance obligations imposed upon Company pursuant to applicable Data Protection Laws, and to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data.
- D. Except as otherwise expressly set forth in the Main Agreement between the Parties, the provision of Services shall be governed by this Agreement pursuant to applicable Data Protection Laws and this Agreement is hereby incorporated into the Main Agreement by reference.

## 1. DEFINITIONS

The following expressions are used in this Agreement. Terms not defined herein have the meaning ascribed to them in the Main Agreement. In the event the definitions herein differ from the Main Agreement relating to data protection, this Agreement shall prevail as to the specific subject matter of such definition.

- a. “Adequate Country” means a country, territory, or specified sectors within a country and international organization published by the European Commission in the Official Journal of the European Union for which it has decided that an adequate level of protection is ensured.
- b. “Data Subject Request” means a request from or on behalf of a Data Subject relating to access of, or the rectification of, erasure of or data portability of that person’s Personal Data or an objection from or on behalf of a Data Subject to the Processing of his or her Personal Data.
- c. “Data Protection Laws” means all laws and regulations applicable to the Processing of Personal Data under the Main Agreement, including but not limited to the GDPR.
- d. “GDPR” means Regulation (EU) 2016/79 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 (known as the General Data Protection Regulation).
- e. “EU Standard Contractual Clauses” means the standard data protection clauses for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR, pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010.

- f. "Personal Data" shall have the meaning given to it by applicable Data Protection Laws.
- g. "Personal Data Breach" means a Personal Data breach as defined under applicable Data Protection Laws that is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data within Plannuh's scope of responsibility by any of its staff, sub-processors or any other identified or unidentified third party after Plannuh becomes aware with a reasonable degree of certainty that such Personal Data Breach has occurred.
- h. "Process", "Processing", "Controller", "Processor", "Data Subject", "Supervisory Authority" or "National Authority" shall have the meanings given to them by GDPR.
- i. "Services" refers to the application, product or services and other activities to be supplied or carried out by or on behalf of Company/Company Affiliate pursuant to the Main Agreement.

## 2. STATUS OF THE PARTIES

2.1 Company is the Data Controller and Plannuh is the Data Processor. Accordingly, Company grants Plannuh the right to Process the Personal Data for the purposes of providing the Services to Company. Plannuh agrees that it shall Process all Personal Data in accordance with its obligations in performing the Services pursuant to this Agreement and the Main Agreement.

## 3. PROCESSING REQUIREMENTS

3.1 *Data Processing Details.* The type of Personal Data Processed pursuant to this Agreement as well as the subject matter, nature and purpose of the Processing, the Data Subjects involved, and the location(s) and duration of the Processing (details required by GDPR Article 28(3)) are as described in the Data Processing Details (Annex 1).

3.2 *Processing under Control of Controller.* Plannuh shall only Process the Personal Data to provide the Services and shall act only in accordance with Company's documented instructions to the extent appropriate for the provision of the Services, and except as required to comply with a legal obligation to which Plannuh is subject. Company's individual instructions on Processing of Personal Data shall be as detailed in the Main Agreement and this Agreement.

3.3 *Confidentiality.* Without prejudice to any existing contractual arrangements between the Parties, Plannuh shall treat all Personal Data as strictly confidential. Plannuh shall take appropriate steps so that only authorized personnel who are subject to binding obligations of confidentiality, either contractual or statutory, will have access to the Personal Data. Termination or expiration of this Agreement shall not discharge Plannuh from its confidentiality obligations.

3.4 *Limitation of Access.* Plannuh will ensure the performance of the Services according to this Agreement is limited to the personnel performing the Services under the Main Agreement.

3.5 *Data Subject Requests.* As between the Parties, Company shall be responsible for addressing all Data Subject Requests. Plannuh shall promptly notify Company if Plannuh receives a request from a Data Subject to exercise his or her Data Subject's rights. Taking into account the nature of the Processing, Plannuh shall assist Company by implementing and maintaining appropriate technical and organization measures in fulfilment of Company's obligations to respond to said Data Subject Request under applicable Data Protection Laws. To the extent legally permitted, Company shall be responsible for any costs arising from Plannuh's provision of such assistance.

3.6 *Notice of Personal Data Breach.* Plannuh maintains an Incident Management Policy and shall notify Company of any Personal Data Breach without undue delay.

In the event of a Personal Data Breach, Plannuh shall identify the cause of such Personal Data Breach and take the necessary steps to remediate the cause of such breach and provide Company with the information describer in Article 33(3) GDPR. Plannuh shall not be responsible for incidents that are caused by Company or Company's end users.

3.7 *Deletion of Personal Data.* Upon Company's written request, or as after termination of this Agreement or the Main Agreement, Plannuh shall delete all Personal Data, except to the extent applicable law requires Plannuh to continue to store the Personal Data. Company acknowledges that Plannuh's deletion of Personal Data represents compliance with any legal obligation to return Personal Data to Company.

3.8 *Audit and Records.* Subject to reasonable prior notice from Company, Plannuh shall provide Company with evidence to demonstrate Plannuh's compliance with this Agreement and Data Protection Laws and shall allow for and contribute to audits, including inspections, conducted by an appropriately certified independent auditor. Company's right of audit under Data Protection Laws may be satisfied by Plannuh through Plannuh providing to Company:

- a. an audit report not older than 12 months by a registered and independent external auditor demonstrating that Plannuh's technical and organizational measures described in the description of Technical and Organizational Measures (Annex 2) are sufficient and in accordance with an accepted industry audit standard such as SOC 2 or ISO27001; and/or
- b. additional information in Plannuh's possession or control to a Supervisory Authority when it requests or requires additional information in relation to the data processing activities carried out by Plannuh under this Agreement.
- c. If Plannuh is unable to provide the information in (a) and (b) above, Company may audit Plannuh's control practices. Company shall reimburse Plannuh for any time expended for any such audit at Plannuh's then-current services rates, which shall be made available to Company upon request. Before the commencement of any such on-site audit, Company and Plannuh shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Company shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Plannuh. Company shall promptly notify Plannuh with information regarding any noncompliance discovered during the course of an audit and allow reasonable time for remediation.
- d. The Parties agree that when carrying out audit procedures relevant to the protection of Personal Data, the Company shall take all reasonable measures to limit any impact on Plannuh's usual course of business operations.

## 4. SECURITY

Taking into account the most recent available technology, 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, Plannuh will maintain appropriate technical and organizational protections as set forth in the description of Technical and Organizational Measures (Annex 2).

## 5. SUB-PROCESSING

5.1 *Cloud Services Sub-Processor.* Company grants Plannuh a specific authorization to appoint the cloud services provider for the Services specified in Annex 4.

5.2 *List Available.* A list of all sub-processors approved by Company above is included in the Sub-Processor List (Annex 4).

5.3 *Sub-Processor Changes; Company Right to Object.* Plannuh will notify Company of the names of any new and replacement sub-processors prior to them beginning sub-processing of Personal Data. Within ten (10) business days of receiving notice of a sub-processor change, Company may object by providing written notice to Plannuh. The notice shall describe the basis for Company's objection, which must have reasonable grounds. Failure to notify an objection during such time period shall constitute waiver of the right to object. If Company gives written notice of objection, Plannuh and Company will discuss the objection in good faith to seek to resolve it. If no objection by Company, the Sub-Processor List (Annex 4) is deemed amended to include the sub-processor identified in the notice.

## 6. DATA TRANSFERS

6.1 *Plannuh Hosting Location.* Plannuh provides, operates, and maintains its Subscription Services in the locations described in the Data Processing Details (Annex 1).

6.2 *Transfer outside EEA, Switzerland and UK by Company.* If, in connection with this Agreement, any Personal Data that is provided by Company from the EEA, Switzerland or the UK to Plannuh outside the EEA, UK, Switzerland and an Adequate Country, such transfer will be governed by the EU Standard Contractual Clauses (Annex 3).

6.3 *Transfers outside the UK or EEA.* Plannuh may transfer Personal Data to Affiliates and other sub-processors operating outside the UK or EEA. If, in the performance of this Agreement, Plannuh has obtained Company's approval to transfer Personal Data outside the UK or EEA (and not to an Adequate Country), Plannuh shall ensure that a mechanism to achieve adequacy in respect to the Processing is in place, such as:

- a. The requirement for Plannuh to execute, for itself and/or, subject to prior consultation, on behalf of Company, Standard Contractual Clauses, as set forth in the EU Standard Contractual Clauses (Annex 3). Upon request, Plannuh will provide to Company for review such copies of agreements, subject to redaction for confidential commercial information not relevant to the requirements under this Agreement.
- b. The existence of any other specifically approved safeguard for data transfer under Data Protection Laws or a European Commission finding of adequacy.

## 7. GOVERNING LAW

Without prejudice to the Standard Contractual Clauses this Agreement shall be governed by and construed in all respects in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

Should any provision of this Agreement be invalid or unenforceable, then the remainder of the Agreement shall remain valid and in force. The invalid or unenforceable provisions shall be either (i) amended as necessary to ensure their 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.

## 8. MISCELLANEOUS PROVISIONS

10.1 *Limitation of Liability.* Company's remedies and Plannuh's liability arising out of or related to this Agreement will be subject to those limitations and exclusions of liability that apply to Company under the Main Agreement to which this Agreement relates. As between the Parties, in no event shall Plannuh be responsible for any liability arising from Plannuh's compliance with Company's instructions.

10.2 *Order of Precedence.* To the extent that any provisions of this Agreement conflict with any provisions in the Main Agreement, this Agreement shall prevail as to the specific subject matter of such provisions; provided, however, that any limitations and exclusions of liability in the Main Agreement and any indemnification provisions in the Main Agreement shall in any event prevail over any provision of this Agreement. If Plannuh provides this Agreement in more than one language for the country of your billing address, and there is a discrepancy between the English text and the translated text, the English text will govern.

### ***EXECUTED BY THE PARTIES AUTHORIZED REPRESENTATIVES***

**Plannuh, Inc.**

**Controller**

Signature



Signature

Name: Peter Mahoney

Name

Title: CEO

Title

Date

## ANNEX 1 – DATA PROCESSING DETAILS

(a) The Data Exporter is Company or an Affiliate of Company or Data Controller, subject to the terms of this Agreement;

(b) The Data Importer is Plannuh or Data Processor, as defined in this Agreement;

(c) The categories of Data Subjects are employees, agents, or contingent workers of Company (who are natural persons);

(d) The nature and purpose of the Processing is delivery of the Services to Company in accordance with Plannuh's published product information. This includes permitting Data Subjects authorized by Company to access Plannuh's Subscription Services in order to manage and update Company's marketing plan, marketing budget, and marketing expenses, stored in Plannuh. To optimize product performance, Company permits Plannuh and its sub-processors to use, compile (including statistical models), annotate and otherwise analyze the data to develop, train, tune, enhance, and improve the benchmarking, forecasting, recommendation and other components of Plannuh's software and technologies embodied in the Subscription Services;

(e) The subject matter of the Processing is the Company's marketing plan, marketing budget, and marketing expenses;

(f) The types of Personal Data involve information necessary for the Data Subject to create an account and use the Services. Personal Data is provided by the Data Subject in order to gain account access and to use the Services, including but not limited to:

Data Subject contact information, meaning personal information normally exchanged during the account creation and usage of a business-to-business (B2B) application, such as name and email address. Because Plannuh is a B2B application, the email address provided is typically the Data Subject's work email address. Company is responsible for instructing and authorizing Data Subjects to provide this personal information in order to access Plannuh;

(g) Processing of Personal Data will be conducted in the following locations:

For Companies in the European Union, in the EU;  
For Companies in the rest of the world, in the USA;

(h) The duration of the Processing is the duration of the Agreement and any data retention period specified therein or under applicable law.



## **ANNEX 2 – TECHNICAL AND ORGANIZATIONAL MEASURES**

### **Security Organization, Risk Analysis and Risk Management**

Plannuh's security organization is headed by the Chief Technology Officer. It works to provide robust information security controls for Plannuh products and environments. Plannuh will perform annual assessments of the compliance of Plannuh security controls with industry standard controls.

### **Workforce Clearing, Training and Sanctions**

All Plannuh personnel are subject to background checks before access to restricted data is permitted. All personnel receive regular security training. Plannuh has adopted policies and procedures to apply workforce sanctions to employees who fail to comply with Plannuh security policies and procedures.

### **Physical Controls**

Cloud Data Center - Amazon Web Services runs in data centers managed and operated by Amazon. These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The data centers are managed, monitored, and administered by AWS operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity. For additional information, please refer to: <https://aws.amazon.com/compliance/data-center/controls/>

### **Access**

Personal Data collected from Data Subjects by Plannuh is protected by encryption and/or multi-factor authentication. Plannuh will only allow employees and contingent workers with a business purpose to have access to such data if it is required for them to complete their professional duties.

### **Business Continuity, Disaster Recovery**

Plannuh has implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services in a timely manner after a disruptive event. Plannuh regularly tests and monitors the effectiveness of its business continuity and disaster recovery plans.

### **Network Security**

All data is protected by encryption in transit over open, public networks. Data at rest is protected by encryption or compensating security controls.

### **Portable Devices**

Plannuh will not store Personal Data on any portable computer devices unless it is encrypted in accordance with then current industry best practice.

### **Monitoring**

Plannuh takes appropriate steps to monitor the security of Personal Data.



## ANNEX 3 – STANDARD CONTRACTUAL CLAUSES

### STANDARD CONTRACTUAL CLAUSES (PROCESSORS) For the transfer of personal data to a Plannuh entity established in a third country which does not ensure an adequate level of data protection

Name of the data exporting organization: Company, as defined in this Agreement.



And

Name of the data importing organization: Plannuh, as defined in this Agreement.

**Plannuh, Inc., 831 Beacon Street #451, Newton Center, MA 02459, USA**

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

### Clause 1

#### Definitions

- a. "Personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in EU Data Protection Laws;
- b. The "data exporter" means the entity who transfers the personal data.
- c. The "data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of EU Data Protection Laws;
- d. The "sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract; and
- e. "Technical and organizational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

### Clause 2

#### Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## Clause 3

### Third-party beneficiary clause

- a. The data subject can enforce against the data exporter this Clause, Clause 4(a) to (j), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- b. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- c. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- d. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

## Clause 4

### Obligations of the data exporter

The data exporter agrees and warrants:

- a. That the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of Data Protection Laws (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b. That it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with Data Protection Laws and the Clauses.
- c. That the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract.
- d. That after assessment of the requirements of the Data Protection Laws, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. That it will ensure compliance with the security measures.
- f. That, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of EU Data Protection Laws;

- g. To forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension.
- h. To make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. That, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j. That it will ensure compliance with Clause 4(a) to (i).

## Clause 5

### Obligations of the data importer

The data importer agrees and warrants:

- a. To process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. That it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred.
- d. That it will promptly notify the data exporter about:
  - i. Any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.
  - ii. Any accidental or unauthorized access; and
  - iii. Any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so.
- e. To deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred.
- f. At the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g. To make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

- h. That, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent.
- i. That the processing services by the sub-processor will be carried out in accordance with Clause 11.
- j. To promptly send a copy of any new sub-processor agreement it concludes under the Clauses to the data exporter.

## Clause 6

### Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.
3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
4. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

## Clause 7

### Mediation and jurisdiction

- a. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - ii. to refer the dispute to the courts in the Member State in which the data exporter is established.
- b. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

## **Clause 8**

### **Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under Data Protection Laws.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under Data Protection Laws.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

## **Clause 9**

### **Governing law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

## **Clause 10**

### **Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

## **Clause 11**

### **Sub-processing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated

at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## Clause 12

### Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

#### *On behalf of the data exporter*

Name (in full): \_\_\_\_\_

Position: \_\_\_\_\_

Address: \_\_\_\_\_

Signature: \_\_\_\_\_

#### *On behalf of the data importer*

Name (in full): Peter Scott Mahoney

Position: Chief Executive Officer

Address: 831 Beacon Street #451, Newton Center, MA 02459, USA

Signature: 

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Defined terms used in this Appendix 1 shall have the meaning given to them in the Agreement (including the DPA).

**Data exporter** - The data exporter is the legal entity specified as "Customer" in the DPA

**Data importer** - The data importer is Plannuh, Inc.

**Data subjects** - Please see Annex 1 of the DPA, which describes the data subjects.

**Categories of data** - Please see Annex 1 of the DPA, which describes the categories of data.

**Special categories of data**- The parties do not anticipate the transfer of special categories of data.

**Purposes of Processing** - Plannuh, Inc. shall process personal data as necessary to provide the Services to data exporter in accordance with the Agreement.

**Processing operations** - Please see Annex 1 of the DPA, which describes the processing operations.


### DATA EXPORTER

Name \_\_\_\_\_

Authorized Signature \_\_\_\_\_

### DATA IMPORTER

Name Peter Mahoney, CEO

Authorized Signature 



## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

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

Please see Annex 2 of the DPA, which describes the technical and organizational security measures implemented by Plannuh.

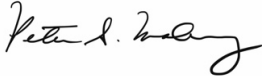
### DATA EXPORTER

Name \_\_\_\_\_

Authorized Signature \_\_\_\_\_

### DATA IMPORTER

Name Peter Mahoney, CEO

Authorized Signature 

## ANNEX 4 – LIST OF SUB-PROCESSORS

Plannuh has engaged and authorized the following types of sub-processors to support the delivery of the Services: consulting firms providing information technology and security advisory and support services; cloud services provider; third party data center operators; customer relationship management software-as-a-service providers and providers of outsourced technical support services.

<b>Sub-Processor Name</b>	<b>Product or Service</b>	<b>Purpose of Data Processing</b>
Amazon Web Services, Inc	Cloud infrastructure services	Hosting of Plannuh application and application data
Waverley Software	Software development and testing	Supports development and testing of core application functionality
HubSpot	CRM cloud services	Provides CRM for relationship with Company; platform for customer support ticketing system for customers
AppCues	In-app user guidance	Provides in-app customer notifications and guidance
Google Analytics	Site usage statistics	Provides Plannuh with app usage statistics