# Teamup Data Processing Agreement

April 12, 2021

## 1. Introduction

Processing personal data in a secure, fair, and transparent way is extremely important to us at Teamup. We process personal data in accordance with the EU's General Data Protection Regulation ("GDPR") and the data protection laws of Switzerland.

This Data Processing Agreement ("DPA") documents how Teamup processes Personal Data on your behalf. It is designed to fulfill GDPR's requirement for a written agreement between Data Controller and Data Processor regarding the processing of Customer's Personal Data.

The latest version of this document is always available at https://www.teamup.com/dpa/.

This version of the DPA replaces the previous version as of May 25, 2018. The main changes are the following:

- Introduced the EU Standard Contractual Clauses (SCC) as the legal basis for the transfer of personal data to the US. SCC replace the EU/US Privacy Shield framework.
- Updated the list of sub-processors used by Teamup.

## 2. Execution

This DPA amends and supplements our Terms of Service and our Privacy Policy and requires no further action on your part. It becomes effective when you start using the Teamup service and accept our terms.

If you do not agree to this DPA, you may discontinue the use of Teamup and delete your calendar.

If you require a signed copy of this document, please contact Teamup at support@teamup.com.

## 3. Definitions

"**Teamup**," "**we**," "**us**," or "**our**" refers to the provider of the Teamup website and services.

"**Customer,**" "**you,**" "**your**" refers to the individual or organization that signs up to use the Service.

"**ToS**" refers to the Terms of Service.

"**DPA**" refers to this document, the Data Processing Agreement.

"**Party**" refers to Teamup and/or the customer depending on the context.

"**Service**" refers to the service provided by Teamup and as set forth in the ToS.

"**EU Data Protection Legislation**" or "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council 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the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (as amended or superseded).

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Data Subject**" means a natural person whose Personal Data is collected or processed.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"**Processor**" means an entity which processes Personal Data on behalf of the Controller.

"**Security Incident**" refers to any breach of the security and/or confidentiality as set out in this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data.

"**Special Category Data**" refers to particularly sensitive Personal Data that falls within the definition of "special categories of data" under EU Data Protection Legislation. This includes for example information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, sexual orientation or criminal records.

"**Standard Contractual Clauses**" or "**SCC**" refer to the model contracts created by the EU Commission for the legal and secure exchange of personal data from within the European Economic Area (EEA) to "third countries" (non-EEA countries).

## 4. Relationship with ToS

4.1 Except as amended by this DPA, the ToS will remain in full force and effect.

4.2 If there is a conflict between the ToS and this DPA, the terms of this DPA will control.

4.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the ToS.

## 5. Roles and Responsibilities

5.1 Parties' Roles: Customer, as Controller, appoints Teamup as a Data Processor to process the Personal Data described in Annex A on Customer's behalf.

5.2 Confidentiality: Each party agrees that Personal Data shall be treated as confidential information under this DPA.

5.3 Ownership: Personal Data shall remain the property of the disclosing party.

5.4 Prohibited Data: Customer will not provide (or cause to be provided) any Special Category Data to Teamup for processing under the ToS, and Teamup will have no liability whatsoever for Special Category Data, whether in connection with a Security Incident or otherwise.

5.5 Description of Processing: A description of the nature and purposes of the processing, the types of Personal Data, categories of Data Subjects, and the duration of the processing are set out further in Annex A.

## 6. Responsibilities of Teamup

6.1 Restrict processing: Teamup will process Customer's Personal Data only to the extent strictly necessary for the purpose of providing the services in accordance with the ToS, any further instructions from the customer given in writing or through the Service, and in accordance with applicable laws.

6.2 Data protection: Teamup will implement and maintain a reasonable and appropriate security program comprising adequate security, technical and organizational measures to protect against unauthorized, unlawful or accidental processing, use, erasure, loss or destruction of, or damage to Customer Personal Data. The technical and organizational security measures which Teamup shall have in place under the ToS are set out in Annex B to this DPA.

6.3 Limit sharing of Personal Data: Teamup will not publish or disclose any Customer Personal Data to any third party with the exception of sub-processors as defined in section 8 "Sub-Processing."

6.4 Limit access to Personal Data: Teamup will ensure that only its personnel who "need-to-know" will be given access to Personal Data to the extent necessary to perform its obligations under the ToS. It shall provide adequate training to its staff and ensure that they comply with the obligations in this DPA.

6.5 Confidentiality: Teamup will ensure that any person that it authorizes to process the Personal Data shall be subject to a duty of confidentiality (whether a contractual or a statutory duty).

6.6 Data retention and export: Upon termination of Customer's use of the Service Teamup will delete the Personal Data and calendar data, in accordance with our standard backup and retention policy, no later than 90 days after the termination. Teamup makes available to Customer tools to export calendar data in a format that allows it to be imported into other services.

6.7 Assistance with compliance: Teamup will assist the Customer by implementing appropriate technical and organizational measures, insofar as this is reasonably and commercially possible, in fulfilling Customer's obligations under applicable data protection laws.

## 7. Responsibilities of Customer

7.1 Customer is a data controller: Customer is in control of what data is made available to the Service. Customer understands, as a controller, that it is responsible for obtaining the consent of

Data Subjects for the processing of Personal Data, for determining the lawfulness of any processing, for performing any required data protection impact assessments, and for accounting to regulators and Data Subjects, as may be needed.

7.2 Rights to Personal Data: Customer warrants that it has all necessary rights to provide to Teamup the Personal Data for processing in connection with the provision of the Teamup Service.

7.3 Parental consent: Customer will make a reasonable effort to verify parental consent when data is collected on a data subject under 16 years of age.

7.4 Measures to protect the data: Customer will implement their own appropriate measures to ensure and demonstrate processing of Personal Data in accord with this DPA and data protection laws.

## 8. Sub-processing

8.1 Sub-processors: Customer agrees that Teamup may engage Teamup affiliates and third party sub-processors (collectively, "Sub-processors") to process Personal Data on Teamup's behalf. The Sub-processors currently engaged by Teamup and authorized by Customer are available at Annex C and online at https://www.teamup.com/dpa/.
Customer may receive notifications of new Sub-processors by e-mailing dpa@teamup.com with the subject “Subscribe”. If a Customer subscribes, Teamup shall provide Customer with notification of new Sub-processor(s) before authorizing such new Sub-processor(s).

8.2 Objection to Sub-processors: Customer may object in writing to the appointment of an additional Sub-processor within ten (10) calendar days after receipt of Teamup's notice in accordance with the mechanism set out at section 8.1 above. In the event that Customer objects on reasonable grounds relating to the protection of the Personal Data, then the parties shall discuss commercially reasonable alternative solutions in good faith. If no resolution can be reached, Teamup will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected Teamup service in accordance with the termination provisions of the ToS.

8.3 Sub-processor obligations: Where a Sub-processor is engaged by Teamup as described in this section, Teamup shall:

(a) impose on such Sub-processors the requirement to comply with GDPR.

(b) establish a DPA with the Sub-processor on substantially the same terms as this DPA.

(c) restrict the Sub-processor’s access to Personal Data only to what is necessary to perform the subcontracted services.

(d) remain liable for any breach of the DPA caused by a Sub-processor.

## 9. International Transfers

9.1 Teamup will exclusively host Personal Data:

(a) in the European Economic Area

(b) in countries designated by the European Commission as providing an adequate level of protection for Personal Data. Read more.

(c) in a third country if the Sub-processor hosting the data has committed to comply with GDPR and the Standard Contractual Clauses.

## 10. Incident Management

10.1 Notification: When either party becomes aware of a Security Incident that impacts the processing of Personal Data, it shall promptly notify the other about the incident and shall reasonably cooperate in order to enable the other party to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

10.2 Mitigation: In case of a Security Incident, each party shall take appropriate and commercially reasonable steps to mitigate the effects of such a Security Incident on the Personal Data under this ToS.

## 11. Cooperation

11.1 Cooperation and Data Subjects' rights: Teamup shall, taking into account the nature of the processing, provide reasonable assistance to Customer insofar as this is possible, to enable Customer to respond to requests from a data subject seeking to exercise their rights under EU Data Protection Legislation. In the event that such a request is made directly to Teamup, Teamup shall promptly inform Customer of the same.

11.2 Data Protection Impact Assessments: Teamup shall, to the extent required by EU Data Protection Legislation and at Customer's expense, taking into account the nature of the processing and the information available to Teamup, provide Customer with commercially reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under EU Data Protection Legislation.

## 12. Security Reports and Audits

12.1 Compliance information: Teamup will make available to the Customer information reasonably necessary to demonstrate compliance with Teamup's obligations under this DPA.

12.2 Customer requests: Teamup shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm Teamup's compliance with this DPA.

# 13. Signatures

13.1 **Customer**

Name: _____

Address: _____

Email: _____

Tel: _____

Date: _____ Signed: _____

**13.2 Teamup**

| | |
|---|---|
| Name: | Teamup Solutions AG, Jenny Zhan Sidler, CEO |
| Address: | Kreuzstrasse 42, 8008 Zürich, Switzerland |
| Email: | dpa@teamup.com |
| Tel.: | +41 44 364 40 37 |

Date: April 12, 2021 Signed: _____

ANNEX A

# DESCRIPTION OF PROCESSING

## 1. Nature and Purposes of Processing

Teamup provides a cloud-based calendar service aimed at facilitating the collaboration of groups. The service is accessible through a web client, a native client for iOS devices, a native client for Android devices and an application programming interface.

Teamup is used in a broad range of use cases. Examples are event calendars, reservation of resources, scheduling and dispatching of resources, absence and availability calendars, etc.

Teamup offers features to:

- enter, update and delete calendar appointments.
- view, print, search, filter calendar appointments in various ways.
- receive notifications about changes to the calendar and upcoming events. Notifications are delivered by email, Slack notifications, mobile push notifications and other transports.
- share calendar appointments with other calendaring applications.
- export and import calendar data.
- synchronize calendar data with other calendaring products.

The content of the calendar is determined by the Customer in its sole discretion.

## 2. Categories of Data Subjects

Teamup collects Personal Data from three categories of Data Subjects:

- Calendar administrators: Calendar administrators create calendars, configure calendars, determine which other users have access to the calendar and determine the use case of the calendar.
- Calendar users: Calendar users are invited by calendar administrators to use the calendars. They receive the necessary credentials to access the calendar from the calendar administrator. Calendar users use the calendar for the use case determined by the calendar administrator.
- Other users: The calendar may be used to collect Personal Data of users that are not themselves using the calendar.

## 3. Categories of Data

Teamup in its role as Controller collects the following Personal Data:

- From calendar administrators if using the free plan: Email address, name (optional), image (optional).

- From calendar administrators if using a paid plan: Email address, name, address, organization name (optional), credit card details, image (optional).
- From calendar users: Email address (optional), name (optional), image (optional).

Teamup in its role as Data Processor processes the following data:

- Any Personal Data that the Customer chooses to enter into the calendar. Teamup has no control over the type, volume and sensitivity of Personal Data collected by the Customer.

## 4. Special Category Data

Teamup does not collect or process any Special Category Data in the provision of its service.

Under this DPA, Customer agrees not to provide Special Category Data to Teamup at any time.

## 5. Duration of Processing

The Personal Data will be processed for the term of the ToS, or as otherwise required by law or agreed between the parties.

ANNEX B

# TEAMUP SECURITY MEASURES

## 1. Data Protection

The protection of your data is our highest priority. We have built a fully redundant, highly available, secure and state-of-the-art technical infrastructure to host your data.

Our servers are hosted in data centers operated by Amazon Web Services. Read more.

## 2. Encryption

Whenever your data is in transit between you and us, everything is encrypted and sent using HTTPS. Data at rest (stored on disk) is encrypted. Any files which you upload to us are stored and are encrypted at rest. Our backups of your data are encrypted.

Data in active use in our database is not encrypted. Access to the database is highly restricted to the server administration personnel needed to maintain systems.

## 3. Redundancy

Our servers operate at full redundancy. This includes power supplies, disks, Internet connections, cooling systems and even entire servers. All data is stored on multiple redundant disks instantly, replicated to multiple independent data centers and backed up daily. Our infrastructure is engineered to stay available even if any one component fails.

## 4. Physical Security

Only authorized personnel have access to the data centers. Round-the-clock onsite security staff as well as interior and exterior surveillance monitoring provides additional protection against unauthorized entry and security breaches.

## 5. Regularly Updated

Our software infrastructure is updated regularly with the latest security patches.

## 6. Billing Information

All credit card transactions are processed using secure encryption—the same level of encryption used by leading banks. Credit card information is transmitted directly between customer and our payment provider Stripe. Teamup does not see, collect, or store your credit card details.

# ANNEX C
# TEAMUP LIST OF SUB-PROCESSORS

Teamup uses the following Sub-processors to provide its service. They have access to some Personal Data as detailed below:

To provide the Teamup calendaring service:

- Amazon Web Services - Server hosting
- Filestack - Document upload
- Google - Traffic analytics
- MailChimp - Newsletter mailing
- Datadog - Log aggregation
- Stripe - Payment solution

To respond to Customers' support requests:

- Help Scout - Help desk solution
- Google - Help desk archive and backup

# ANNEX D

# GDPR Standard Contractual Clauses

Annex D contains the Standard Contractual Clauses SCC provided by the European Union in the context of GDPR. SCC establish the legal basis for the transfer of personal data to processors located in third countries which do not ensure an adequate level of data protection. Teamup includes the SCC in this DPA because several of its sub-processors are established in the United States. All sub-processors of Teamup are required to comply with the SCC as well.

## Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

**Data exporting organization (the data exporter):**

The Customer, See section 13.1 of the DPA

And

**Data importing organization (the data importer):**

Teamup, see section 13.2 of the DPA

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

For the purposes of the Clauses:

a. ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the

European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b. ‘the data exporter’ means the controller 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 Article 25(1) of Directive 95/46/EC;

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;

e. ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f. ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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(b) to (i), 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 the applicable data protection law (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 the applicable data protection law and the Clauses;

c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 Directive 95/46/EC;

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 organisational 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 unauthorised access; and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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 send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## Clause 6

## Liability

a. 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.

b. 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 of by operation of law, in which case the data subject can enforce its rights

against such entity.The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

c. 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

a. 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 the applicable data protection law.

b. 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 the applicable data protection law.

c. 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

a. 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 fulfil 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.

b. 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.

c. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

d. 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(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

a. 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.

b. 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.

# Appendix 1 to the Standard Contractual Clauses

This Appendix includes certain details of the processing of personal data as required by Article 28(3) GDPR forms and part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Teamup is a general purpose scheduling tool and caters to a broad customer and end user base that spans across the spectrum of industries. Teamup does not control nor limit the subject matter our customers' end users submit through the use of our tool. Considering this, the nature of the product, and Teamup's role as a processor, inventorying an absolute list of data categories ingested and processed is not possible.

**Data exporter**

The data exporter is the entity identified as "Customer" in the DPA or "you" in the Terms of Service.

**Data importer**

The data importer is Teamup Solutions AG.

**Data subjects**

Data subjects include the data exporter's customers and end-users.

**Categories of data**

Annex A, section 3 of the DPA documents the categories of data collected and processed by Teamup.

**Special categories of data (if appropriate)**

Teamup explicitly prohibits the use of its service for the processing and storage of Special Category Data (see section 5.4 of this DPA).

**Processing operations**

Personal data will be processed in accordance with the Terms of Service (including this DPA) and may be subject to the following processing activities:

Storage and other processing necessary to provide, maintain and improve the Teamup service provided to customer pursuant to the Terms of Service; and/or

a. Disclosures in accordance with the Terms of Service and/or as compelled by applicable law.
b. Nature and purpose of processing: Personal Data is processed for the purpose of delivering the Teamup service as more particularly described in this DPA.

Duration and subject matter of processing: The subject matter and duration of the processing of the personal data are set out in the Terms of Service.

Personal Data Deletion or Return: Upon expiration or termination of the data exporter's use of the Services, the data importer will delete or return the Personal Data in accordance with the terms of the Terms of Service(including this DPA).

## Appendix 2 to the Standard Contractual Clauses

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

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

See Annex B of this DPA.