Teamup Data Processing Agreement

August 20, 2023

1. Introduction

Processing personal data in a secure, fair, and transparent way is extremely important to us at Teamup. This Data Processing Agreement ("DPA") documents how Teamup processes Personal Data on your behalf.

Teamup processes your Personal Data in accordance with:

- the California Consumer Privacy Act (the "CCPA")
- the General Data Protection Regulation of the European Union ("GDPR")
- the General Data Protection Regulation of the United Kingdom ("UK GDPR")
- the Federal Act on Data Protection of Switzerland ("FADP")

This document supplements our Terms of Service. It incorporates the following additional documents:

- Standard Contractual Clauses between controllers and processors approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "SCCs"). The SCCs apply if the GDPR, the UK GDRP, or the Swiss FADP apply to your use of Teamup.
- Teamup CCPA Terms if the CCPA applies to your use of Teamup
- UK Addendum to the DPA if the UK GDPR applies to your use of Teamup
- Swiss Addendum to the DPA if the Swiss FADP applies to your use of Teamup
- Teamup Operations & Security describes in detail how Teamup protects Customer data.

The latest version of this document is always available at https://www.teamup.com/dpa/. A PDF version of this document optimized for printing is available here.

2. Execution

This DPA 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 for your record, 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.

“**CCPA**” refers to the California Consumer Privacy Act of 2018 as amended, including as amended by the California Privacy Rights Act of 2020, together with any implementing regulations.

“**FADP**” refers to the Swiss Federal Act on Data Protection.

"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).

“**Data Protection Legislation**” refers to GDPR, UK GDPR, Swiss FADP, or CCPA, whichever is applicable to Customer.

"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 that 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).

“**Third Country**” means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

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

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

(c) 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.

9.2 Application of Standard Contractual Clauses

The Standard Contractual Clauses will only apply to Customer Data subject to the GDPR that is transferred, either directly or via onward transfer, to any Third Country (each a "Data Transfer").

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 applicable 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 applicable 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 applicable 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: August 20, 2023 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, and 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 administrators select the subscription plan and for paid subscriptions arrange the payment using a credit card, bank transfer or other online payment system.
- 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 Customer 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 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, entire servers, data center buildings, and data centers. 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 provide 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 several sub-processors to provide its service. The following list shows all sub-processors with access to some Personal Data.

To provide the Teamup calendaring service:

- Amazon Web Services - Server hosting
- Filestack - Document upload
- MailChimp - Newsletter mailing
- Datadog - Log aggregation
- Stripe - Handling of subscription payments

To respond to Customers' support requests:

- Help Scout - Help desk solution

ANNEX D
Document History

Aug. 20, 2023	● Incorporated the latest version of the Standard Contractual Clauses as of September 24. 2021. ● Added the Swiss Addendum to the Data Processing Agreement ● Added the UK Addendum to the Data Processing Agreement ● Added the Teamup CCPA Terms ● Rewrote the introduction ● Minor adjustments in various sections
April 12, 2021	● 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.
May 25, 2018	● First version