Data Processing Agreement

Contract on the collection, processing, and/or use of personal data
in accordance with Art. 28 of General Data Protection Regulation (GDPR), status as of: 09.08.2022

Preamble

The present data processing agreement addresses central points related to collecting, processing, and/or using personal data. The contracting parties agree that this contract only contains data protection regulations for order processing.
The obligations described above apply to all activities that relate to the service contract and in which the employees of the service provider (IWOP GmbH, Albert-Einstein-Str. 1, 49076 Osnabrück, Germany) or third parties commissioned by the service provider may encounter personal data of the service recipient (the company that creates a user account at www.teamlove.app).

1. Subject and duration of the order (first sentence of Art. 28(3) GDPR)

1.1. The subject of the order is the collection and analysis of opinion data of employees, customers, suppliers, or business partners of the service recipient by the service provider in the context of using the team feedback tool "Teamlove" by the service recipient.

1.2. The duration of the order (term) begins with the creation of a user account on the website www.teamlove.app by the service recipient and ends with the deletion of the user account by the service recipient or the service provider for reasons specified in the GTC. The contract is valid regardless for as long as the service provider processes the personal data of the service recipient (including backups).

2. Scope and type of data collection (first sentence of Art. 28(3) GDPR)

2.1. To provide the service of Teamlove, the service provider requires access to the data under 2.2. Access is required in particular for the following points: Creating a user account for employees or other persons who are to participate in the team feedback, sending invitations via e-mail addresses to participate in the team feedback, assigning account holders to teams, companies, and departments or groups of teams, collecting the opinion data of the team members, assisting with the evaluation of the feedback result and the achievement of objectives. The use of anonymized data for scientific research by the service provider is permitted.

2.2. As part of using Teamlove by the service recipient, the service provider collects, processes, and uses self-declared opinion data (e. g. attitudes, evaluations, assessments), communication data (e. g. e-mail addresses for communication and setting up accesses) as well as work-related metadata (e. g. organizational unit, position) of the participants. Necessary communication and personnel master data for the implementation of the team feedback tool are collected independently by the service recipient and made available to the service provider for processing and use via input masks in the Teamlove user interface.

2.3. Those affected by the handling of their data are usually employees of the service recipient but may also be customers, suppliers, or business partners, depending on the composition of the teams created by the service recipient in Teamlove.

3. Implementation and compliance with technical-organizational measures

3.1. Within their area of responsibility, the service provider takes all necessary technical and organizational measures according to Art. 32 GDPR on the protection of personal data and provides the service recipient with the documentation of these measures for review [Appendix 1]. The documented measures shall become the basis of this contract.

3.2. Insofar as the review/audit by the service recipient reveals a need for adaptation, this must be implemented by mutual agreement, or the use of Teamlove by the service recipient must be discontinued.

3.3. The agreed technical and organizational measures are subject to technical progress and further development. In this respect, the service provider is permitted to implement adequate alternative measures in the future. This must not fall below the safety level of the measures laid down. The service recipient shall be informed immediately of any significant changes, which are to be documented by the service provider.

4. Rights and requests of data subjects

4.1. The responsibility for safeguarding the rights of the persons affected by the data storage by the service provider (particularly concerning requests for correction, deletion, blocking, and provision of information) lies with the service recipient. The service provider shall support the service recipient in their area of responsibility and, as far as possible, in responding to and implementing requests from data subjects regarding their data protection rights.

4.2. The service provider may not disclose, port, correct, delete, or restrict the processing of data processed on their own authority, but only in accordance with the contractual agreement or the instructions of the service recipient.

4.3. Insofar as a person concerned contacts the service provider directly in this regard without existing agreements or instructions from the service recipient, the service provider shall immediately forward this request to the service recipient.

4.4. To the extent covered by the scope of services, the erasure concept, the right to be forgotten, correction, data portability, and information shall be ensured directly by the service provider in accordance with the documented instructions of the service recipient.

5. Obligations of the service provider (Art. 28(3) GDPR)

5.1. In addition to compliance with the provisions of this agreement, the service provider has legal obligations according to Art. 28 to 33 GDPR; in this respect, they ensure particularly compliance with the following requirements:

5.1.1. Written designation of a data protection officer who carries out his/her activities in accordance with Art. 38 and 39 GDPR, to the extent required by law. The contact details are: Heiko Beemers, TopZert GmbH, Stader Landstr. 27a, 21762 Otterndorf, Germany,

Phone: +49 4751 999 54 69, datenschutz@topzert.eu. The service recipient will be notified promptly of any change regarding the data protection officer.
5.1.2. Maintaining confidentiality in accordance with the second sentence of Art. 28(3)(b), Art. 29, Art. 32(4) GDPR. The service provider shall only use employees in the performance of the Work who have been committed to confidentiality and have been familiarized in advance with the data protection provisions relevant to them. The service provider and any person subordinate to the service provider who has access to personal data may process such data exclusively by the instructions of the service recipient, including the powers granted in this agreement, unless they are required to process it by law.

5.1.3. The service recipient and the service provider shall cooperate with the supervisory authority in the performance of their duties upon request.

5.1.4. The immediate information of the service provider about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies to the extent that a competent authority investigates the service provider's processing of personal data during order processing in the context of an administrative offense or criminal proceeding.

5.1.5. Insofar as the service recipient is subject to an inspection by the supervisory authority, administrative offense, or criminal proceedings, the liability claim of a data subject or a third party, or any other claim in connection with the order processing by the service provider, they shall support the service provider to the best of their ability.

5.1.6. The service provider regularly monitors the internal processes as well as the technical and organizational measures to ensure that the processing in their area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.

5.1.7. Proof of the technical and organizational measures taken vis-à-vis the service recipient within the scope of their control powers.

6. Subcontracting relationships

6.1. For the purposes of this regulation, subcontracting relationships shall be understood as services that relate directly to the collection and analysis of data. This does not include ancillary services used by the service provider, such as telecommunications services, postal/transport services, maintenance and user service, disposal of data carriers, and other measures to ensure the confidentiality, availability, integrity, and resilience of the hardware and software of data processing systems. However, the service provider is obligated to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the service recipient's data, even in the case of outsourced ancillary services.

6.2. The service provider may engage carefully selected subcontractors to fulfill the contractual agreements. When engaging subcontractors, the service provider must observe the requirements pursuant to Art. 28(2-4) GDPR and design the contracts so that they comply with the framework conditions described in this agreement.

6.3. The service recipient agrees to the subcontractors referred to in 15.1 under the condition of a contractual agreement with the subcontractors pursuant to Art. 28(2-4) GDPR.

6.4. If the service recipient objects to the establishment of a subcontracting relationship, they have a special right to termination. They may delete their user account on Teamlove at any time and thus terminate the order processing. The special right of termination has priority over other agreements regarding terms and termination rights.

6.5. The transfer of personal data of the service recipient to subcontractors and their first activity are only permitted after all requirements for subcontracting have been met.

7. Control rights of the service recipient

7.1. The service recipient has the right to conduct inspections in agreement with the service provider or to have them carried out by inspectors to be appointed in individual cases. The service recipient shall have the right to verify the service provider's compliance with this agreement in their business operations during usual business hours by means of spot tests, which must generally be notified in good time.
7.2. The service provider ensures that the service recipient can convince themselves of the service provider's compliance with their obligations pursuant to Art. 28 GDPR. The service provider undertakes to provide the service recipient with the necessary information on request and to provide evidence of the implementation of the technical and organizational measures.

8. Support by the service provider

8.1. The service provider supports the service recipient in complying with the obligations regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments, and prior consultations set out in Art. 32 to 36 GDPR. These include, but are not limited to:

8.1.1. Ensuring an adequate level of protection through technical and organizational measures that consider the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible infringement due to security holes and allow for immediate detection of relevant breach events.

8.1.2. The obligation to immediately report personal data breaches to the service recipient.

8.1.3. The obligation to support the service recipient in their obligation to inform the data subjects and to provide them with all relevant information in this context without delay.

8.1.4. The support of the service recipient for their data protection impact assessment.

8.1.5. The support of the service recipient in the context of prior consultations with the supervisory authority.

9. The service recipient's power to direct (second sentence of Art. 28(3)(a) GDPR)

9.1. The service recipient shall immediately confirm verbal instructions in writing or by e-mail (in text form).

9.2. The data shall be handled exclusively within the scope of the agreements made and according to the instructions of the service recipient. The service recipient reserves the right to give comprehensive instructions on the type, scope, and procedure of data processing within the scope of the order description agreed in this agreement, which they may specify by means of individual instructions. Changes to the subject of processing and changes to procedures must be jointly agreed upon and documented. The service provider may only provide information to third parties or the data subject with the prior written consent of the service recipient.

9.3. The service provider must inform the service recipient immediately if they believe that an instruction violates data protection regulations. The service provider is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the service recipient.

9.4. Instructions shall be kept by the service recipient for their period of validity and thereafter for three full calendar years.

9.5. The service recipient shall inform the service provider immediately if errors or irregularities are detected during the examination of the order results.

10. Deletion of data and return of provided data carriers (second sentence of Art. 28(3)(g) GDPR)

10.1. The service provider shall not use the data for any purposes other than those described in this document and shall particularly not be entitled to disclose them to third parties. Copies or duplicates of the data shall not be made without the knowledge of the service provider. This does not include (security) copies insofar as they are necessary to ensure proper data processing and data required regarding compliance with statutory retention obligations.

10.2. The deletion of data ensued in compliance with data protection requirements upon request (in writing or text form) by the service recipient.

10.3. There is no provision for the exchange of data carriers. In exceptional cases, the data carriers provided are returned to the service recipient.

11. Remuneration

11.1. The service provider shall have a claim to remuneration for services that go beyond obligations to comply with the GDPR, and which are not due to their fault, but which have been commissioned by the service recipient. The service provider shall inform the service recipient in advance in text form (e. g. e-mail) about the chargeability and, as far as possible, about the estimated effort. The costs shall be invoiced according to the daily rate agreed in the service contract.

12. Relationship to the General Terms and Conditions (GTC)

12.1. Insofar as no special provisions are contained in this agreement, the provisions of the GTC of the service provider shall apply.

12.2. In the event of contradictions between this agreement and provisions from other agreements, particularly from the GTC, the provisions from this agreement shall prevail.

13. Final provisions

13.1. Amendments and additions to this Agreement and all of its components - including any assurances by the service provider - must be made in writing and must expressly state that they are an amendment or addition to these Terms and Conditions. This also applies to the waiver of the formal requirement.

13.2. Should individual parts of this contract be or become invalid, this shall not affect the validity of the rest of the contract. The ineffective part shall be replaced by mutual agreement by such a provision that comes as close as possible to the original intention of the parties in terms of economics and data protection.

13.3. In the event of any gaps in the provisions, the Parties shall make a provision that they would have made if they had considered the relevant point when concluding the Agreement.

13.4. The place of jurisdiction and applicable law shall be governed by the GTC.

14. Liability

14.1. The service recipient and the service provider are liable to data subjects in accordance with the provisions of Art. 82 GDPR.

15. List of subcontractors

Salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 München, Germany
Stripe, Inc., 354 Oyster Point Blvd, South San Francisco, CA 94080, United States
Google Commerce Limited, Gordon House, Barrow Street, Dublin 4, Ireland
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Germany

Technical-organizational measures

In accordance with Art. 32(1) GDPR

Date: 04. Jul 2022 **Date of the last change:** 09. Aug 2022

1. General framework conditions

The Provider points out that the following technical and organizational measures are subject to technical progress and further developments and that alternative adequate measures can also be applied, whereby significant changes are communicated and documented.

2. Confidentiality (Art. 32(1)(b) GDPR)

Confidentiality as part of information security - appropriate measures that ensure that information is only accessible to a specific group of recipients.

2.1. Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

The service provider does not operate its own data centers, but rents web servers from carefully selected third-party providers for the purpose of conducting and automatically evaluating surveys. Due to the nature of the service, reference is made in particular to the data center operators for access control. These are generally certified according to ISO/IEC 27001 and provide the rented server in a European data center.

The access control to the business premises of the service provider is basically irrelevant for the provision of Teamlove, since no data is stored here or separate access possibilities to the data exist. For completeness, it is nevertheless described below: The ICO, where the Service Provider has its corporate headquarters, is secured from the outside and inside as follows: There are triple windows in the building that cannot be fully opened. There are no light shafts or ventilation openings through which unauthorized persons could possibly gain access to the offices. There is no video surveillance. There are motion detectors in the publicly accessible corridor areas.

Only authorized persons have access to the ICO. On weekdays, the main entrance door is also open to visitors from approx. 07:30 to 18:00. In the evening, the closing of the doors is controlled by a security service. The cleaning staff has access to the premises in principle, but has signed a declaration to this effect, which can be viewed at the ICO if required. A transponder system is used as a key in the ICO building. The transponders are of the type that they cannot be easily duplicated without authorization. The data of access to each door is stored for the last 200 accesses. The accesses to the main entrance door outside the main opening hours are always recorded.

The offices in the center of Osnabrück are secured from the outside and inside as follows: Access to the offices is protected by lockable security and steel doors. The door to the outside area can only be opened from the outside with a key. The doorbell system has an intercom function. In addition, access can be further secured by a lockable rolling gate. The triple windows of the office rooms can be locked manually or electronically and are not very visible due to their location facing the inner courtyard. Motion detectors are used in the outdoor area and in the offices. There is no video surveillance either outside or in the offices. If external persons need access to the offices, they are constantly accompanied by employees of IWOP GmbH. There are smoke detectors and fire extinguishers in the offices.

All keys to office rooms of IWOP GmbH are listed in an overview document. Both the issue and the return of keys are acknowledged. The keys of employees who have left the company are collected immediately. Surplus keys are deposited in a safe.

2.2. Logical Access Control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

After the creation of participant data by the service recipient in the user interface of Teamlove, personal data is only permanently stored on the web server. This data remains on the web server until it is deleted and is automatically evaluated on the web server. No other data carriers in the actual sense are used. This process architecture limits the possibilities for data access and makes them easier to control. The server protection is decisive for ensuring admission control. This is done via a secure shell in combination with public key authentication. Unrestricted access to the server database is possible only after logging on to the server. The database access is protected in the second step by a username/password combination. Protection of other non-public services is done by means of authentication by username and password. Within the framework of data protection and IT security of the service provider, a password policy exists for the secure use of passwords according to the state of the art. Passwords are managed in an encrypted password file (256-bit AES in combination with a passphrase). Firewall-, intrusion- and prevention systems and anti-malware or anti-virus software are used to further secure the web server. Documentation is provided via an internal wiki and ticket system.

2.3. Authorization Control

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

All data provided by the service recipient and all data collected as part of the survey will be treated confidentially. This is ensured by an authorization concept: The number of administrators and access rights is reduced to a minimum. Access authorizations for employees are limited to those persons involved in software development or administration and are immediately blocked or deleted by the system administrators if necessary (e.g., at the end of an employee's contract). Database accesses such as the entry, modification or deletion of entries are logged. The deletion of data carriers is done for root servers by multiple overwriting and the subsequent decommissioning of the server. If there are any other documents or data carriers that need to be destroyed, they will be transported in sealed containers to a carefully selected, certified disposal company with a written commitment to data protection, where they will be disposed of in accordance with data protection regulations.

2.4. Separation Control

Measures to ensure that data collected for different purposes can be processed separately.

The service provider operates separate systems for development and productive use; there is no logical client separation. Data records are provided with purpose attributes to ensure the correct allocation of data.

Communication and opinion data are stored in independent database tables. To ensure anonymity in the feedback process, feedback results are never reported with a personal reference. Within the teams, however, the open comments entered are reported in plain text and may possibly allow conclusions to be drawn about individual persons. This procedure is mandatory for working with the results. At the company level, no comments from individual persons are presented, but only problem and action areas defined jointly by teams.

3. Integrity (Art. 32(1)(b) GDPR)

Integrity as part of information security - appropriate measures that ensure the correctness/integrity of data and the correct functioning of systems.

3.1. Transfer Control

Measures to ensure that personal data cannot be read, copied, modified or removed by unauthorized persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Transport security of data is ensured using Transport Layer Security (TLS, formerly SSL). When creating and integrating the encryption certificates, the configuration parameters recommended by the Mozilla Corporation for "Intermediate compatibility" are used to establish the highest possible security while ensuring a high level of compatibility with client systems. A list of allowed algorithms can be provided.

The exchange of personal data always takes place in encrypted form via the Teamlove server. Data exchange via transport of physical or electronic data carriers between the service provider and the server recipient does usually not take place.

3.2. Input Control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered, modified, or removed from the data processing systems.

The entry of opinion data as part of the feedback process is only carried out by the concerned persons themselves. The entries can be revised within one feedback cycle, after which a change is no longer possible. The input of personal data in the context of the creation of teams, including the team administrators, is carried out by the service recipient itself. Changes are to be documented by the service recipient and are not logged in the system. The entry of personal data in the context of inviting team members is carried out by the team administrator of the service recipient. Changes must be documented by the team administrator and are not logged in the system.

4. Availability (Art. 32(1)(b) GDPR)

Availability as part of information security - appropriate measures that ensure that IT systems meet their requirements within the expected time.

4.1. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

Data availability is always guaranteed by selecting data center operators certified in accordance with ISO/IEC 27001. These offer protection against fire, smoke, lightning, gas, and water damage. The data center rooms are air-conditioned and equipped with an emergency power supply. Only redundant storage systems are used for data storage. These enable the replacement of individual damaged storage media without data loss during ongoing operation. In addition to these measures, database backups are made daily.

5. Resilience

Description of measures that ensure the resilience, insensitivity, and defense of systems against software defects, extreme number of requests, viruses, hacker attacks, etc.

Due to the system architecture used, the entire process of data collection and data evaluation takes place on the server. Basically, the server capacity is adapted to the requirements of the project. The server is monitored both manually and via automated administrator notifications for the status of key performance data such as accessibility/latency and CPU, disk, and memory utilization. However, should a resource bottleneck occur, we have various options for load balancing as well as additional allocation of server power. Firewalls, intrusion prevention systems, and anti-malware or anti-virus software are also used to secure the web server.

6. Recoverability Control (Art. 32(1)(c) GDPR)

Description of the measures that ensure the restoration of the functionality of the IT systems within a reasonable time after a system failure.

The survey server is installed and set up using an automated configuration and software management tool. Even after a complete failure of the productive system, a new server configuration including all security and performance relevant settings can be set up as quickly as possible, a back-up of the database can be imported, and the system can be restored to its original state. The first point of contact for technical problems should always be Teamlove's customer service.

7. Procedures of regular Review, Assessment, and Evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

Description of the documented arrangements for periodic review and updating of information security.

7.1. Order Control

Measures to ensure that personal data processed on behalf can only be processed in accordance with the instructions of the service recipient.

The handling of personal data is carried out in accordance with the legal guidelines and in accordance with the instructions of the service recipient, who can suggest legally compliant (GDPR, BDSG-new, and other applicable data protection regulations) changes to the type, scope, and procedure of data processing. The employees of the service provider are obligated to maintain data secrecy and sign corresponding instructions. Subcontractors are carefully selected. Checks are carried out on-site or by means of documents provided, such as certificates or deeds. Responsibilities are clearly defined for the implementation of projects in cooperation with other partners or subcontractors.

The monitoring-, firewall-, intrusion prevention and anti-malware systems log relevant events and are regularly evaluated in terms of information security status.