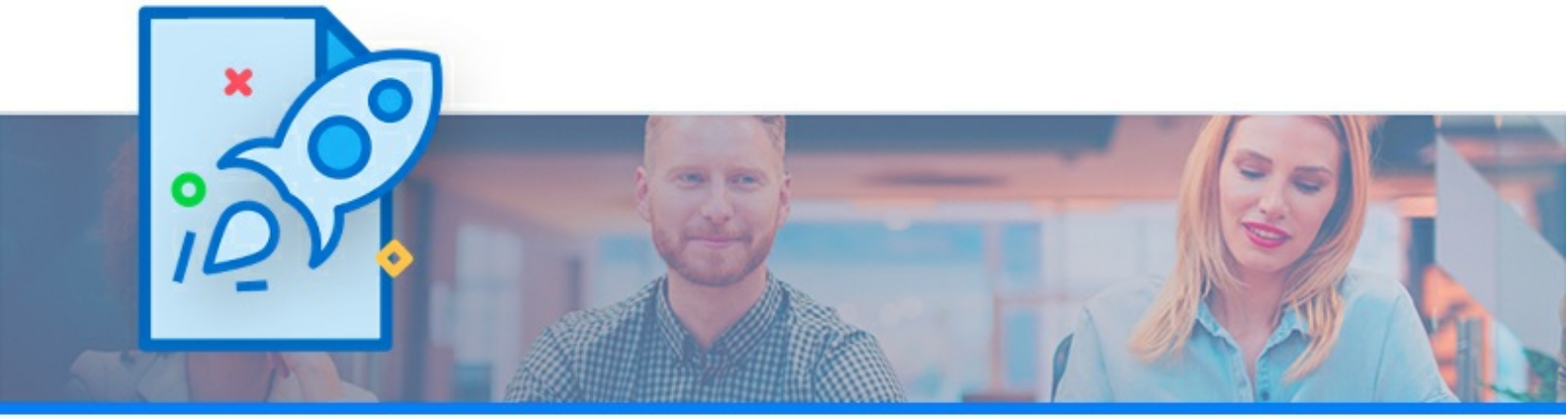
Data Processing Agreement

between
UberGrape GmbH
Lange Gasse 76/18, 1080 Vienna, Austria
FN 405900m

and
[Controller.CompanyName]
[Controller.CompanyAddress]
represented by [Controller.Name]

On the [Document.CreatedDate]



DEFINITIONS

Controller	Controller means [Controller.CompanyName] with its business address [Controller.CompanyAddress], represented by [Controller.Name]
Processor	This Contract is a contract according to Art 28 of the GDPR. Processor means UberGrape GmbH (Brand Name: "Grape"), an Austrian limited liability company, with its seat in Vienna and its business address Lange Gasse 76/18, 1080 Vienna, registered with the Vienna Commercial Court under registry number FN 405900m.
Grape	The product that the Processor is offering

Preamble

1. **Processor**. The Processor operates a project messenger software as a service („Product“).
2. **Principal Contract**. The Parties made an agreement over the use of the Product (https://www.chatgrape.com/terms-of-service/) (the „Principal Contract“). This contract amends the Principal Contract.
3. **Subject**. In fulfillment of the Principal Contract the Processor processes personal data of the Controller and of the Controller’s employees, freelancers and similar contributors of content, in each case at the Controller’s order. This Contract regulates rights and obligations of the Parties concerning the fulfillment of the Principal Contract.
4. **Processor**. This Contract is a contract according to Art 28 of the GDPR.

ART I. Definitions

1. In this Contract, except where a different interpretation is necessary in the context, capitalized terms shall have the meaning assigned to them in the section entitled "Definitions" set forth in Schedule § I.1.

ART II. Details of the Processing

1. **Subject**. The subject of this Contract is the provision of the Product.
2. **Categories of Data**. For the provision of the Product the categories of data listed in Schedule § II.2 (the „Data“) are processed.
3. **Way and Purpose**. The Processing is performed in the way and for the purposes described in Schedule § II.3.
4. **Categories of Data Subjects**. The Processing concerns categories of Data Subjects as set forth in Schedule § II.4.
5. **Duration**. This Contract is binding for the duration of the Principal Contract. During the duration of the Principal Contract this Contract can only be terminated for good reason. If the Principal Contract is terminated by a Party this Contract ends automatically. The obligation pursuant to § V.2 continues to exist even in case of termination.

ART III. Place of Processing

1. The Processing of Data partially takes place outside the EU and the EEA. Countries, in which the Processing takes place, and the basis for an appropriate level of data security are listed in Schedule § III.1.

ART IV. Rights and Obligations of the Controller

1. **Assignment**. The Controller is a Controller within the meaning of Art. 4 sec 7 GDPR and has instructed the Processor with the Processing of Data.
2. **Right to Information**. The Controller has the right to receive all information required to prove compliance with the Processor’s obligations listed in Art. Error: Reference source not found and to perform reviews, including inspections, by himself or through an assigned investigator.

ART V. Rights and Obligations of the Processor

1. **Processing**.
    1. The Processor will process Data solely upon the Controller’s prior written instruction. This also applies to (i) the transfer of Data to a third country or to an international organization and (ii) the Processing of Data for the Processor’s own purposes.
    1. § V.1(a) does not apply to the Processing of Data, if the Processor is legally obliged to

do so. In these cases the Processor informs the Controller about its obligation before Processing, if no important public interest prohibits such information.

2. **Data Confidentiality**. The Processor and his coworkers are obliged to maintain data confidentiality pursuant to Art 6 of the Austrian Data Protection Act in the version of May 25, 2018. The Processor must contractually bind his employees to maintain data confidentiality, if they are not legally obliged to do so already. This obligation has to remain in effect even if the employment relationship is terminated. The Processor declares to comply with these obligations.
3. **Technical and Organisational Measures**.
    1. The Processor declares explicitly to have taken the necessary measures to obtain security of Processing of Data according to Art. 32 GDPR. A complete list of those measures can be found in Schedule § V.3(a) (the "Measures").
    2. Should any change of the Measures reduce the safety standard regarding the Processing of Data, the Processor will coordinate these changes with the Controller.
    3. The Controller has the right to be informed about the actuality of the Measures and to obtain a copy of the current version of those Measures by the Processor.
4. **Support of the Controller**.
    1. The Processor will support the Controller as far as possible, by taking appropriate technical and organizational measures, to fulfill the Controller's obligation of responding to the requests of data subjects according to Art. 3 GDPR. Should such a request have been sent to the Processor instead of the Controller by accident, the Processor shall forward it to the Controller immediately and inform the applicant about this proceeding.
    2. The Processor shall, considering the nature of the processing and information available, support the Controller to fulfill its obligations under Art. 32 to 36 GDPR (guaranteeing the security of Processing, notifications or communications to the supervisory authority or data subjects, data protection impact assessment including prior consultation).
5. **Processing after Termination**. When the Processing of Data is finished, the Processor shall, depending on the Controller's decision, either return to it or delete all Data. This does not apply, if the Processor is legally obliged to store the Data.
6. **Obligation to Inform**. The Controller ensures the execution of the right to information pursuant to § IV.2.
7. **Unlawful Instructions**. The Processor will inform the Controller promptly, if it considers an instruction to be unlawful under the data protection legislation of the EU or applicable law of member states.
8. **Record of Processing Activities**. The Processor keeps a record of Processing activities pursuant to Art. 30 GDPR.

ART VI. Sub-Processor

1. **Right to Engage Sub-Processors**. The Processor has the right to engage another Processor for the operation of the Product (a “Sub-Processor”), including the Processing of Data, without the Controller’s previous consent. In the case of an intended change regarding the Sub-Processor, the Processor will inform the Controller in due time.
2. **List of Sub-Processors**. A list of all currently engaged Sub-Processors can be found in Schedule § VI.2.
3. **Obligations**. In case a new Sub-Processor is engaged, the Processor concludes all required agreements according to Art. 28 sec 4 GDPR with the Sub-Processor. These agreements must bind the Sub-Processors to the same data safety obligations as determined in this Contract, especially concerning guarantees for appropriate technical and organizational measures.
4. **Liability**. If a Sub-Processor does not comply with its data safety obligations, the Processor is fully responsible for the compliance with these duties to the Controller.

ART VII. Final Provisions

1. The clauses in Schedule § VII.1 concerning governing law, form, and other regulations stated therein are applicable.

Vienna, on the [Document.CreatedDate]

UberGrape GmbH

_____ _____

Name: [Processor.Name]
Title: [Processor.Role]

[Processor.CompanyName]

_____ _____

Name: [Processor.Name]

Schedule § I.1
Definitions

GDPR	GDPR means the EU-regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Processing	Processing means Processing of Data according to Art. 4 Z2 GDPR.

Schedule § II.2
Categories of Data

1. Communication data: userid, timestamp and content of messages sent on Grape.
2. User/employee data

Schedule § II.3
Type and Purpose

1. Types of Processig: collection, storage, organization, transmission, recording, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by dissemination or otherwise making available, alignment or combination, restriction, erasure and desctruction
2. Purposes of Processing:
    1. Fulfillment of the Principal Contract
    2. customer relations management (e.g. support);
    3. marketing for our own products (newsletters)
    4. personalizing your experience of the Services
    5. research and development
    6. communicating with you about the Services
    7. market, promote and drive engagement with the Services
    8. ensuring safety and security
    9. protecting our legitimate business interests and legal rights.

Schedule § II.4
Categories of Data Subjects

Users who report a bug
[Controller.DataSubjectsEmployees]
[Controller.DataSubjectsCustomers]
[Controller.DataSubjectsOther]

Schedule § III.1
List of Countries for Data Processing incl. Foundations

1. Austria
2. Germany
3. Ireland
4. USA, based on the EU-US Privacy Shield pursuant Article 45 GDPR

Schedule § V.3(a)
Measures

1. **Pseudonymization/Encryption.**
    1. Google Analytics: IP Anonymization
    2. Encryption of passwords for integrations in our database, if the integration requires us to authenticate with a password. Otherwise OAuth and similar techniques are used.
2. **Confidentiality**
    1. Entrance Control
        1. Servers in secure GDPR compliant datacenter with biometric access control and video surveillance 24/7
        2. Office
            1. Secure lock on the main door.
            2. Visitors are only let in if a person inside the company has invited them and is responsible.
            3. Security Camera filming the entrance
            4. No critical hardware in the office, all stationary computers have full-disk encryption enabled.
    2. Admission Control.
        1. Access to servers only via SSH key file. No other access method.
        2. Website server physically separated from product servers
        3. Grape testing servers physically separated from Grape production servers and have only dummy data
        4. Configuration for production server (secret keys etc.) separated from code, versioned in Git only encrypted. Not available to developers.
    3. Access Control.
        1. Processes for on-boarding and off-boarding employees and external staff, including giving them only necessary permissions on all affected systems.
        2. Access groups, based on teams, with individual permissions for people on all used
        3. systems.
        4. Regular checks where permissions and/or access is removed for individuals if not

needed anymore
5. Deployments are verified via Developer's SSH key.

3. **Integrity.**
    1. Input Control.
        1. Administrative actions in the Admin-area are logged with the userid and timestamp
        2. Code changes and configuration changes are logged in Git with the username, email and timestamp
        3. Deployments to all servers are logged into our internal chat and into a separate log file with userid and timestamp.
    2. Transfer Control.
        1. Communication to Grape servers is only possible via TLS (HTTPS/WSS), except for the redirect to HTTPS. HSTS headers are in place.
        2. Certificate pinning in the iOS App
        3. Data sent from Grape servers to sub-processors is only done over TLS.
4. **Availability/Resilience.**
    1. Linux system hardening process with Operations Team
    2. Stateful firewall on all servers
    3. Two-hourly backups of all databases, daily copy to a physically separated backup server. Additionally, GPG encrypted backups are copied daily to another server in a different location, at a different hosting provider.
    4. Security report page to contact the processor to report an incident or vulnerability (GPG Email public key available for security researchers): https://www.chatgrape.com/report/
    5. Patching of very severe vulnerabilities (CVSS score 9-10) within 48 hours of a patch release for the operating system, the Grape code and for containers.
    6. White-Box Code audits are done on request by external companies
    7. Internal and external monitoring of main services, with alerting and employee on-call duty planning.
5. **Restoration/Destruction.**
    1. Restoration: All necessary data for restoration is in the backup. Recovery of our backups has been successfully tested. A full recovery takes 4 hours.
    2. Destruction:
        1. Backups are deleted after two months automatically.
        2. The controller can delete the whole organisation on his own, with no steps required from the processor. Individual users will be deleted automatically when synced via AD.□ Manually managed users can be removed by the Controller with no steps required from the Processor.
6. **Review.**
    1. Assignment Control.

1. Data is only processed as instructed by the Controller in the Terms of Service and this Contract.
2. The controller can export his organisation's data (except private messages and groups) and delete his organisation's data at any time (self-service)

2. Miscellaneous.
    1. An incidence response plan is documented and a part of the team has been trained in detail how to properly respond to security incidences.
    2. A head of data protection has been appointed, see Privacy Policy.

Schedule § VI.2
List of Sub-Processors

1. **Hetzner**: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
2. **Hubspot**: Hubspot Inc, Cambridge, Massachusetts, USA
3. **Google (G-Suite, GCM, Analytics, Adwords)**: Google Dublin, Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland and Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
4. **Pandadoc**: Pandadoc, 153 Kearny Street, San Francisco, California, USA
5. **Fabric**: Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd.
6. **Apple (APNS)**: Apple Inc., Cupertino, Kalifornien, Vereinigte Staaten
7. **Microsoft (WPM)**: Microsoft Corp., Redmond, Washington, Vereinigte Staaten
8. **Moreify (SMS)**: IXOLIT GmbH, Mariahilfer Straße 77-79, 1060 Vienna, Austria
9. **Twitter**: Twitter Corp., San Francisco, California, USA
10. **Facebook**: Facebook, Inc., 1601 South California Avenue, Palo Alto, CA 94304, USA
11. **Zendesk**: Zendesk, Inc., 1019 Market Street, 6th Floor, San Francisco, CA 94103, USA
12. **AWS**: Amazon Web Services Inc., 410 Terry Avenue North Seattle, WA 98109-5210, USA

Schedule § VII.1
Final Provisions

1. **Confidentiality**. The Parties agree to handle all information received in relation to the Contract in a confidential way for an indefinite period of time and use this information for the fulfillment of the Contract only. This information shall be used for the referred purposes only and must not be disclosed to third parties. This does not apply, if (a) the obligated Party obtains information demonstrably form a third party, to which it is not obliged to confidentiality, (b) if the information was publicly available or (c) the disclosure was legally required or demanded by the authorities.
2. **Entry into Force**. The Contract enters into force with signing by both Parties and is binding for an indefinite period of time.

3. **Written Form**. Any adjustments, amendments or a revocation of the contract requires written form. or, if the Contract was entered into via electronic means, a similar form to the conclusion of the Contract. This also applies to any regulation intending to change the written form requirement.
4. **Severability**. In the event that individual provisions of this Contract shall be or become invalid or unenforceable, all other terms and conditions shall remain in full force and effect. The parties agree to replace the invalid or unenforceable clause with a valid and enforceable clause, that has the same economic sense. This rule also applies in case a regulatory gap occurs.
5. **Legal Foundation**. Only the provisions of this contract and, additionally, the legal regulations shall apply.
6. **Governing Law**. This Contract and all correlating contractual relations and litigation shall be governed by Austrian law, excluding the conflict of law-provisions of the United Nations Convention on Contracts for the International Sale of Goods.
7. **Court of Jurisdiction**. Exclusive court of jurisdiction for any legal disputes with regards to this Contract shall be, to the extent legally permissible, Vienna, Austria.