



Data Processing Addendum

This Data Processing Addendum, including the Standard Contractual Clauses (as defined below) attached hereto (collectively, the "DPA"), is made and entered into as of the effective date (the "Effective Date") of the applicable client's ("Client") acceptance of the Terms of Service between Gleap GmbH ("Gleap") and Client to which this DPA is attached and incorporated (the "Agreement"). All capitalised terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. Under the Agreement, Gleap provides certain Services to Client that may involve Gleap processing client's data, which may include Personal Information (as defined below).

This DPA forms part of the Agreement and contains certain terms and conditions relating to data protection, privacy and security to include certain requirements of the General Data Protection Regulation (EU) 2016/679 (the "GDPR"), including the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"), and the California Consumer Privacy Act of 2018 (Cal. Civ. Code, Title 1.81.5 comprising §§ 1798.100 – 1798.198 (as amended) (the "CCPA"), where applicable. In the event (and to the extent only) that there is a conflict between the GDPR and the CCPA, the parties agree to comply with GDPR.

1 Preamble

- 1.1 With this contract, the parties mutually regulate their rights and obligations with regard to the processing of personal data for the duration of the order and, if expressly provided for in this contract, beyond the duration of this contract.
- 1.2 In this contract, the Contractor shall provide the guarantees required under Article 28 of the General Data Protection Regulation (hereinafter "**GDPR**") that the processing complies with the requirements of the GDPR and that the protection of the rights of the data subject is ensured by appropriate technical and organizational measures.
- 1.3 This Agreement applies to all activities in which the Contractor, employees of the Contractor or subcontractors engaged by the Contractor (hereinafter referred to as "**Subcontractors**") process personal data of the Client within the scope of the Client's order.
- 1.4 Terms used in this Agreement have the same meaning as defined in the GDPR. The Client / Customer is therefore the "Controller" and the Contractor ("Gleap GmbH") is the "Processor".

2 Subject matter of the contract / duration

2.1 Subject

In order to fulfil the mission agreed between the Parties, the Contractor shall perform the following processing operations:

Bug Reporting, Crash Reporting, Live-Chat-Services, Features Requests-Services, Conduct Surveys, Product Tours, Offer and reply to Chat-Messages (direct communication), Operating Email-communication-Services, Operating Help Center/Support-Services; News and Releases Notes-Services.

The Processing is based on the Service Terms and Conditions concluded between the Parties (hereinafter "Service Terms and Conditions"), as attached hereto as Annex ./2.1. In the Service Contract, the assignment and data processing scope agreed between the Parties is exhaustively enumerated. In case of contradictions between the scope of processing in this Agreement and in the Service Agreement, the more specific provisions in the Service Agreement shall prevail over those in this Agreement]. The Parties agree, to the extent possible, to reduce the amount of data processed/scope of data processed to the extent necessary for the provision of services by the Contractor pursuant to the Service Agreement (reduction of data volumes)].

2.2 Duration

Processing shall commence on the effective date (the "Effective Date") of the applicable client's acceptance of the Terms of Service between Gleap GmbH ("Gleap") and Client to which this DPA is attached and incorporated and shall continue indefinitely until termination of this Agreement or the Service Agreement by either party.

3 Type, purpose and data subjects of the data processing:

3.1 Type of processing

Processing means the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data, as referred to in Article 4(2) of the GDPR.

3.2 Purpose of processing

The underlying purpose of the processing is regulated in the service description of the service conditions, which is attached to this contract as Annex ./2.1.

3.3 Type of personal data

The following data are processed by the contractor:

Personal Data:

(i) Chat messages:

Date;

Message;

Attachment (file, optional);

Session ID;

(ii) Every ticket inquiry comes with the following data:

Form data (depends on what data you collect - typically email & description);

Date created;

Outbound ID (when sent as survey);

Priority of the inquiry;

Status of the inquiry;

Session ID (used to identify the user);

Project ID;
Organization ID;
Screenshot data (for JS);
Replay data;
Steps to reproduce data;
Clicks (used to reproduce the issue);
Metadata (including OS info, browser info);
Attachments (if activated);
Network logs (if activated);
Custom data (this is data set by our customer - we don't know what it includes);
Action log (if set);
Console logs (includes the log of the developer console);

(iii) The Gleap session data includes:

Gleap ID (randomized ID to identify a session);
Gleap Session Hash (Hash that provides proof of identity);
Name (if set with the identify method)
User ID (if set with the identify method)
Email address (if set with the identify method OR through form-data);
Approximated location (the accuracy allows only to identify the country due to anonymization of the IP address);
IP-address (not directly stored but used for rate limiting to protect our infrastructure);
Name (if set with the identify method or extracted from the email address);
Value of the customer;
Custom data (this is data set by our customer - we don't know what it includes);

Only the Gleap ID and Gleap Session Hash are mandatory and generated by default. All other information is optional and depends on the configuration of the customer's project.

- (iv) **Events (Gleap allows customers to track events like "signedUp", "loggedIn" (events are used for debugging purpose & to trigger surveys & outbound messages)**

Date;

Session ID;

Event name;

Custom event data (this is data set by our customer - we don't know what it includes);

3.4 Categories of data subjects

The following persons are affected by the processing by the Contractor:

customers of the Client, interested parties of the Client, employees of the Client, App & Website users of the Client.

4 Obligations of the Client

- 4.1** The Client shall be solely responsible for assessing the permissibility of the processing pursuant to Article 6 (1) of the GDPR and for safeguarding the rights of the data subjects pursuant to Articles 12 to 22 of the GDPR. Nevertheless, the Contractor is obligated to forward all such requests to the Client without delay, provided that they are recognizably directed exclusively to the Client. The Client shall be responsible for ensuring that the processing of personal data with which the Contractor is commissioned is carried out on a legal basis.
- 4.2** Changes to the object of processing and process changes shall be mutually agreed between the parties and set out in writing.
- 4.3** The Client shall place all orders, partial orders and instructions in writing (e-mail fulfils the written form requirement).
- 4.4** Should the Client gain knowledge of the Contractor's trade secret or data security measures during this contractual relationship, the Client undertakes to treat these confidentially. This obligation shall continue to apply even after termination of this contract.

5 Obligations of the Contractor

- 5.1** The Contractor shall process personal data exclusively as agreed in this Agreement or as instructed by the Client. Exceptions apply if the Contractor is legally obligated to a certain processing. If such obligations exist for the Contractor, the Contractor shall inform the Client thereof prior to processing, unless such notification is prohibited by law from the outset. The data provided for processing shall be processed exclusively for the purposes specified in the service agreement. These data shall not be used by the Contractor for any other purposes or for its own purposes.
- 5.2** The Contractor confirms that he is aware of the relevant data protection regulations. The Contractor is committed to the proper processing of data.
- 5.3** The Contractor shall maintain strict confidentiality in the processing of the data.
- 5.4** All persons (in particular employees of the Contractor) who obtain knowledge of the data processed in the order shall undertake in writing to maintain confidentiality, unless they are already subject to a duty of confidentiality regulated in the respective service contract or to statutory duties of secrecy. The list of persons to whom access has been granted shall be reviewed at regular intervals. On the basis of this review, access to personal data may be withdrawn if such access is no longer required; these persons shall consequently have no further access to personal data.
- 5.5** The Contractor warrants that its employees have been familiarized with the relevant provisions of data protection and this Agreement prior to the start of processing. The Contractor shall hold corresponding training and awareness-raising measures for employees on a regular basis. In addition, the Contractor shall ensure that the employees used for the commissioned processing are appropriately instructed and monitored with regard to the data protection requirements on an ongoing basis.
- 5.6** The Contractor shall support the Client in fulfilling its obligations under data protection law. For example, in the creation and updating of the list of processing activities, in the performance of the data protection impact assessment and any necessary consultation with the supervisory authority. The required documents shall be kept available and transmitted to the Client without delay upon request.
- 5.7** If the Client is subject to an inspection or if data subjects assert rights against the Client, the Contractor shall support the Client to the extent necessary. However, this shall only be done to the extent that the processing of the respective order is affected.

- 5.8** The Contractor may only provide information to third parties, or the person concerned with the prior consent of the Client. Inquiries addressed directly to the Contractor shall be forwarded to the Client without undue delay for appropriate response.
- 5.9** As a matter of principle, the commissioned processing shall take place within the EU or the EEA. Any relocation to a third country may only take place with the consent of the client and under the conditions contained in Chapter V of the GDPR and in compliance with the provisions of this contract.

6 Security of the Processing

- 6.1** The Parties agree that the data security measures set out in Annex .6.1 are binding in order to ensure the security of the Processing as defined in Article 32 of the GDPR. The Contractor shall take data security measures appropriate to the respective risk.
- 6.2** The data security measures may be adapted to technical and organizational developments. The Contractor shall implement any changes required to maintain information security without delay. Such changes shall be communicated to the Client without delay. Material changes shall be agreed between the Parties.
- 6.3** If the security measures taken do not or no longer meet the requirements of the Client, the Contractor shall notify the Client without delay.
- 6.4** The Contractor warrants that it strictly separates the data processed in the order from other data files.
- 6.5** No copies or duplicates shall be made without the knowledge of the Client. Technically necessary, temporary duplications are excepted, insofar as an impairment of the level of data protection agreed here is excluded.
- 6.6** The processing of data in private homes is not permitted. The processing of data on behalf of private devices is not permitted under any circumstances.
- 6.7** To the extent required by law, the Contractor shall appoint a competent and reliable person as data protection officer so that the Client can contact the data protection officer directly in cases of doubt (see Annex .6.7).
- 6.8** The Contractor shall provide regular evidence of the fulfilment of its obligations, in particular the complete implementation of the agreed technical and organizational

measures as well as their effectiveness. The Contractor shall provide the Client with this evidence without unnecessary delay and without being requested to do so at the end of each calendar year. Evidence shall be kept for at least three calendar years after the end of the commissioned processing and shall be presented to the Client at any time upon request.

7 Regulations on the correction, deletion and blocking of data

- 7.1** The Contractor shall only correct, delete or block data processed within the scope of the Client's order in accordance with the contractual agreement reached or at the Client's instruction.
- 7.2** The Contractor shall carry out instructions from the Client regarding the correction, deletion or blocking of data at any time, even after termination of this Agreement. The Contractor shall charge a separate fee for such activities after the termination of this Agreement.

8 Subcontracting Relationships (Subcontractors)

- 8.1** The commissioning of further subcontractors (beyond the group of persons listed in Annex ./8.10) shall only be permitted with the written consent of the Client in individual cases. The Client shall not be entitled to refuse consent without justification if the same data protection obligations have been or can be contractually imposed on the subcontractor as correspond to the obligations agreed in this Agreement.
- 8.2** The rights of the Client may also be effectively exercised against subcontractors. The Client shall be entitled to carry out inspections of subcontractors.
- 8.3** The responsibilities of the Contractor and the subcontractor shall be clearly demarcated.
- 8.4** Further subcontracting by the subcontractor is not permitted.
- 8.5** When selecting the subcontractor, the Contractor shall take into account the suitability of the technical and organizational measures taken by the subcontractor.
- 8.6** The forwarding of data processed in the order to the subcontractor shall only be permitted after the Contractor has satisfied itself in a documented manner that the subcontractor has fulfilled its obligations in full. The Contractor shall submit the documentation to the Client upon request and without being asked to do so.

- 8.7** The commissioning of subcontractors who perform processing operations on behalf of the Contractor not exclusively from the territory of the EU or the EEA shall only be possible if the conditions specified in this contract are complied with. In particular, it is only permissible to the extent and as long as the subcontractor provides adequate data protection guarantees. The Contractor shall inform the Client which specific data protection guarantees the subcontractor offers and how proof thereof can be obtained.
- 8.8** The Contractor shall adequately review the Subcontractor's compliance with its obligations on a regular basis, at the latest every 12 months. The inspection and the result shall be documented. The Contractor shall keep the documentation on audits carried out at least until the end of the third calendar year after termination of the commissioned processing and shall submit it to the Client upon request at any time.
- 8.9** Direct liability of the Contractor for the subcontractor is excluded. The Contractor shall only be liable to the Client for the Subcontractors within the scope of the selection fault.
- 8.10** At present, the Subcontractors specified in Annex ./8.10 with name, address and order content are engaged in the processing of personal data to the extent specified therein. The Client expressly gives its consent to this. The other obligations of the Contractor towards subcontractors set forth herein shall remain unaffected.
- 8.11** Subcontracting relationships within the meaning of this contract are only those services that are directly related to the provision of the main service. Ancillary services such as transport, maintenance and cleaning as well as the use of telecommunication services or user services are not covered. The obligation of the Contractor to ensure compliance with data protection and data security in these cases shall remain unaffected.

9 Obligations to notify

- 9.1** In the event of a breach of the protection of personal data processed on behalf of the Contractor, the Contractor shall notify the Client of such a breach without delay. Reasonable suspicions shall also be reported to the Client. The notification shall be made immediately upon the Contractor becoming aware of the relevant event to an address designated by the Client. It shall contain at least the following information:

- (i) a description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of individuals involved, the categories affected, and the approximate number of personal data records affected;
- (ii) the name and contact information of the Data Protection Officer (if any) or other point of contact for further information; and
- (iii) a description of the measures taken or proposed to be taken by Contractor to address the Personal Data Breach.

9.2 Significant disruptions in the execution of the order as well as violations of data protection provisions by the Contractor or the persons employed by it shall also be reported immediately.

9.3 The Contractor shall inform the Client without undue delay of inspections or measures by supervisory authorities or other third parties, insofar as these relate to the commissioned processing.

9.4 The Contractor assures the Client that it will support the Client in its obligations pursuant to Articles 33 and 34 of the GDPR to the extent necessary.

10 Instructions

10.1 The Client shall have a comprehensive right to issue instructions to the Contractor with regard to the processing of data in the course of the order.

10.2 Only the persons named in Annex ./10.2 shall be entitled to issue and receive instructions.

10.3 The Client shall issue instructions in writing (via e-mail). Verbally issued instructions shall be void until they have been issued in writing and addressed to the persons named in Annex ./10.2.

10.4 In the event of a change or a longer-term prevention of the designated persons, the Parties undertake to inform the respective successors or representatives without delay.

10.5 The Contractor shall notify the Client without delay if, in its opinion, an instruction issued by the Client violates statutory provisions. The Contractor shall be entitled to suspend the execution of the respective instruction until it is confirmed or amended by the responsible person at the Client. If the instruction violates legal regulations even after confirmation or amendment, the Contractor shall not be obliged to carry it out.

11 Termination

11.1 If, upon termination of the contractual relationship, processed data or copies thereof which are related to the order are still in the Contractor's possession, the Contractor shall, at the Client's option, either (i) destroy the data or (ii) hand them over to the Client (stored in a manner compliant with data protection requirements on suitable storage media). The Client shall make this choice within two weeks of being requested to do so by the Contractor. If the Client does not make a choice as to whether the data is to be handed over or destroyed, the Client shall destroy the data. The destruction shall be carried out in such a way that a recovery of even residual information is no longer possible with reasonable effort.

11.2 The Contractor shall be obligated to instruct the immediate destruction or return also of subcontractors. The Contractor shall not be liable for the ultimate destruction of the data by the Subcontractors.

11.3 The Contractor shall provide proof of proper destruction and submit it to the Client upon request.

11.4 Documentation which serves as proof of proper data processing shall be kept by the Contractor at least until the end of the third calendar year after the end of the contract. The Contractor may hand them over to the Client earlier for its own relief.

12 Liability

12.1 The Client and the Contractor shall each be individually liable on the basis of the respective principle of fault for compensation for damage suffered by a person due to unauthorized or incorrect data processing within the scope of the contractual relationship. This liability is not to be understood as joint and several or joint and several liability.

- 12.2** The Client shall bear the burden of proof that damage is the result of a circumstance for which the Contractor is responsible, insofar as the relevant data were processed by it under this Agreement.
- 12.3** The Contractor shall only be liable to the Client for damage culpably caused by the Contractor or its employees. Liability for damages caused by slight negligence on the part of the Contractor or its employees is excluded.
- 12.4** The Contractor shall not assume any liability with regard to the execution of unlawful instructions of the Client (item 10.). If the Contractor nevertheless carries out an unlawful instruction of the Client, whether due to insistence of the Client or ignorance of the unlawfulness of the Contractor, and for this reason is liable to a third party, the Client shall in any case indemnify and hold the Contractor harmless.

13 Applicable Law

This Agreement and its legal effect, interpretation and performance shall be governed exclusively by Austrian law, excluding the conflict of laws rules. The possible applicability of the Vienna UN Convention on Contracts for the International Sale of Goods is excluded.

14 Place of Jurisdiction

For all disputes or claims arising from or in connection with this contract or relating to its conclusion, validity, infringement, dissolution or nullity, the court with jurisdiction for commercial matters at the registered office of the Contractor (thus the LG Feldkirch) shall have exclusive jurisdiction.

15 Miscellaneous

- 15.1** Both Parties are obligated to treat all knowledge of business secrets and data security measures of the other party obtained within the framework of the contractual relationship as confidential, even after the termination of the contract. If there is any doubt as to whether information is subject to the obligation of confidentiality, it shall be treated as confidential until it has been released in writing by the other party.
- 15.2** Ancillary agreements to this contract must be in writing and must expressly refer to this contract.
- 15.3** Should individual provisions of this contract be invalid or unenforceable or become invalid or unenforceable after conclusion of the contract, this shall not affect the

validity of the remaining provisions of the contract. The invalid or unenforceable parts of the contract shall be replaced by those provisions whose effects come closest to the economic objective that the contracting Parties pursued with the invalid or unenforceable provisions.

Signatures

The parties agree that execution of the Agreement by the data Processor and the data Controller shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.

Attachments

Annex 6.1 - Technical and organizational measures

Annex ./8.10 - Approved sub-service providers

Annex ./10.2 - Persons authorized to give instructions, address for reporting data protection violations

Attachment./2.1. - Service Agreement

Annex 6.1 – Technical and organizational measures

As agreed in Clause 6, this Annex lists the order-related technical and organizational measures to ensure data protection and data security. These include in particular:

1. pseudonymization (pursuant to Article 32(1)(a) DSGVO in conjunction with Article 25(1) DSGVO) and encryption (pursuant to Article 32(1)(a) DSGVO) of personal data;
2. confidentiality (pursuant to Article 32(1)(b) DSGVO) of the systems and services related to the processing. This includes:
 - a. an access control: no unauthorized access to data processing systems,
 - b. an access control: no unauthorized system use,
 - c. access control: no unauthorized reading, copying, modification or removal within the system, and
 - d. a separation control: separate processing of data collected for different purposes.
3. the integrity (as defined in Article 32(1)(b) of the GDPR) of the systems and services related to the processing. This includes:
 - a. a transfer control: no unauthorized reading, copying, modification or removal during electronic transmission or transport.
 - b. an input check: determining whether and by whom personal data have been entered into, modified or removed from data processing systems.
4. the availability and resilience (pursuant to Article 32(1)(b) of the GDPR) of the systems and services related to the processing. This includes:
 - a. an availability control: protection against accidental or deliberate destruction or loss; and
 - b. a resilience check: the ability of the systems to cope with risk-related changes and to demonstrate tolerance and compensatory capacity in the face of disruptions.
5. the recoverability (Article 32(1)(c) DSGVO) of and access to the personal data;
6. procedures for regular review, assessment, and evaluation (Article 32(1)(d) GDPR; Article 25(1) GDPR) of the effectiveness of technical and organizational measures to ensure the security of processing. This includes:

- a. a data protection management: system for the regular review, assessment and evaluation of data protection measures;
- b. incident response management: system for preparing, identifying and reporting security incidents;
- c. data protection-friendly default settings, and
- d. an order control system.

Annex 6.7. – Data protection officer

Currently appointed as data protection officer at the Contractor is:

Lukas Böhler

lukas@gleap.io

Managing Director, Gleap GmbH

15 years of professional experience in software development, several times in charge of projects with data protection relevant topics.

Annex ./8.10 – Approved Subcontractors

Firma	Anschrift	Auftragsinhalt
Microsoft Azure	Microsoft One Microsoft Way, Redmond, WA 98052, United States +1 425-882-8080 Server location: Germany, Frankfurt	Server (NodeJS, Screenshot Rendering, Redis Database) hosting & static file hosting.
MongoDB	MongoDB Building 2 Number One Ballsbridge, Shelbourne Rd, Ballsbridge, Dublin 4, D04 Y3X9, Ireland Server location: Germany, Frankfurt	Our main database.
Postmark	ActiveCampaign, LLC 1 N Dearborn Street, Suite 500, Chicago, IL 60602 Server location: USA	Email service: We are using this service to send out emails. Postmark is one of the world leaders in the domain of email sending.
OpenAI	OpenAI, L.L.C. 3180 18th St San Francisco, CA 94110 Attn: General Counsel / Copyright Agent dmcanotice@openai.com Server location: USA	This service is used to power our AI features. The AI features are optional and you must not use them. It is also possible to fully disable them. Simply contact us for more information.
CloudFlare	Cloudflare, Inc., located at 101 Townsend St., San Francisco, California 94107 Server locations: Worldwide (static files are distributed world wide to ensure fast loading speeds). No personal data is hosted at CloudFlare.	Static file hosting and DNS management.
Pusher	Pusher Limited Eighth Floor 6 New Street Square, New Fetter Lane, London, England, EC4A 3AQ, Server location: EU, Ireland	Websocket provider, helping us to scale our websockets and delivering our real time features.
Stripe	Stripe, Inc. Corporation Trust Center, 1209 Orange Street, Wilmington, New Castle, DE 19801, USA	Payment provider (customer billing)
Amplitude	Amplitude, Inc., 201 Third Street, Suite 200, San Francisco, CA 94103 Server location: EU	Analytics service to improve our Gleap service.
Firebase	Google Ireland Limited Gordon House, Barrow Street Dublin 4. Ireland	Push notification provider (this feature must be manually activated)
AWS	Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	Server (NodeJS, Screenshot Rendering, Database) hosting & static file hosting.
Digital Ocean	DigitalOcean, LLC. 101 Avenue of the Americas, 10th Floor New York 10013 Server location: EU, Frankfurt	Server (NodeJS, Screenshot Rendering, Database) hosting & static file hosting.

Annex./10.2. – Persons authorized to issue instructions, address for reporting data protection violations

Contact person for reports of personal data breaches:

Lukas Böhler

privacy@gleap.io

Attachment./2.1. - Terms of service

Please find our latest terms of service on our website under:

<https://www.gleap.io/terms-of-service>