Data Processing Agreement under Article 28 GDPR concluded:

between	[Client legal name] [Registered address] [Authorized representative] and Gleap GmbH Am Dorfplatz 3 6858 Schwarzach Austria
represented by	*represented by* Lukas Böhler, Chief Executive Officer (CEO)
hereinafter: „**Client“**	hereinafter: „**Contractor“,** (together with the Client, the „**Parties**““)

Last updated: 20.09.2026

Selected hosting region: EU (Frankfurt) / US (NYC3): _____

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 DPA have the meanings given in the GDPR. The Client acts as Controller and Gleap GmbH (the Contractor) as Processor. If the Client acts as Processor for another Controller, the Contractor acts as its sub-processor and the Client warrants that it is authorized to issue the instructions and grant the authorizations in this DPA on that Controller's behalf.

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:

Customer feedback and support services, including bug and crash reporting, live chat, feature requests, surveys, product tours, email communication, help-center services, news and release notes. Optional AI services include agents, reply assistance, transcription, search and retrieval, knowledge-base ingestion and connected-repository analysis and code assistance, as configured by the Client and described in Annex 8.10.

The service agreement, applicable order and this DPA describe the services and processing. The Client's authorized configuration and use of the service constitute documented instructions within that scope. This DPA prevails for personal-data processing if it conflicts with the service agreement, subject to mandatory law and any applicable Standard Contractual Clauses. A separately negotiated written provision expressly varying this DPA prevails only to the extent legally permitted. Processing shall be limited to what is necessary to provide the configured services.

2.2 Duration

Processing shall commence on the effective date specified in the service agreement or, if none is specified, on execution of this DPA, and shall continue until termination of this DPA or the service agreement.

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 inquery;

Status of the inquery;

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 is responsible for the lawfulness of its personal data and instructions, including the required legal bases, notices and consents, data minimization, and decisions about data-subject requests. The Client shall configure its integrations, masking, access permissions and optional AI features appropriately and shall not submit special-category or criminal-conviction data unless expressly agreed in writing with suitable safeguards. The Contractor shall assist as required by this DPA and applicable law and shall forward requests concerning the Client's data without undue delay. Nothing in this clause removes the Contractor's own statutory obligations.

4.2 Changes outside the agreed services or processing scope, including a migration of existing data between regions, require written agreement on scope, feasibility, timing and any reasonable charges. This does not restrict assistance or other obligations required by applicable data protection law.

4.3 The Client may issue documented instructions through authorized service settings, the applicable order or email to the contacts in Annex 10.2. The Client shall secure its accounts and ensure that persons giving instructions are authorized.

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 Taking into account the nature of processing and the information available to it, the Contractor shall provide reasonable assistance required by Articles 28(3)(e) and (f) GDPR, including data-subject requests, security, breach obligations, impact assessments and prior consultation. The Contractor may charge reasonable, documented fees for assistance beyond standard service functionality, notified in advance, except to the extent required to remedy its own breach or prohibited by law. Urgent statutory assistance shall not be delayed pending agreement or payment of fees.

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 The Client selects the EU or US hosting region at signup or in the applicable order. Customer databases, uploaded files and backups remain in that region: DigitalOcean Frankfurt, Germany, for EU accounts and DigitalOcean NYC3, New York, United States, for US accounts. EU accounts use EU AI endpoints and US accounts use US AI endpoints. The selection is a documented hosting instruction; changing an SDK endpoint does not migrate existing data. A migration requires a further documented instruction and agreement under clause 4.2. Regional storage and AI endpoints do not determine the location of every provider operation, supporting service, remote access or onward transfer. Such processing is limited to the purposes and locations disclosed in Annex 8.10 and remains subject to clauses 8.1, 8.4 and 8.7. Before a transfer subject to Chapter V GDPR occurs, the Contractor shall ensure an applicable adequacy decision or appropriate safeguards, including completed Standard Contractual Clauses where relied upon and supplementary measures where required. An applicable UK transfer instrument shall be used where UK GDPR requires it. Selection of US hosting does not waive statutory rights or constitute reliance on an Article 49 derogation. Existing regional restrictions remain effective until validly amended.

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 Contractor may update technical and organizational measures to reflect technical developments and service changes, provided that the overall level of protection is not materially reduced and Article 32 GDPR continues to be met. Material changes affecting the Client's data protection shall be notified without undue delay. Any departure from expressly agreed minimum protections requires agreement where required by the applicable contract or law.

6.3 If the Contractor becomes aware that the agreed technical and organizational measures no longer meet its obligations under this DPA or Article 32 GDPR, it shall notify the Client without undue delay and take appropriate corrective action.

6.4 The Contractor shall maintain logical separation of customer data and appropriate access controls in its shared service infrastructure. This does not require dedicated physical infrastructure unless expressly agreed.

6.5 The Client authorizes copies reasonably necessary to provide, secure, back up and restore the service, subject to this DPA's purpose, confidentiality, regional storage and retention requirements. Copies shall not be used for unrelated purposes.

6.6 Processing from private homes is permitted only through the Contractor’s VPN using company-managed devices and subject to the access controls and confidentiality obligations of this DPA. Processing on personal devices is prohibited.

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 make available the information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits, including inspections, by the Client or an independent auditor mandated by it. Routine assurance shall first use available independent audit reports, relevant documentation and reasonable written responses under confidentiality. If these do not reasonably resolve a substantiated compliance concern, an appropriately scoped inspection shall be allowed. Routine audits require 30 days' written notice, occur during business hours no more than once per year and are at the Client's expense. Those limits do not apply where a competent authority requires otherwise, following a relevant personal data breach, or where additional audits are reasonably necessary to investigate credible evidence of material non-compliance. The parties shall minimize disruption and protect other customers' data, trade secrets and system security, using redaction or equivalent evidence where appropriate without preventing legally required verification. Auditors shall be suitably qualified, independent and bound to confidentiality. The Contractor may charge reasonable documented assistance costs, except for audits establishing its material breach or where prohibited by law. Mandatory authority powers and statutory audit rights remain unaffected.

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 implement lawful correction, deletion and restriction instructions concerning personal data it still holds, including after termination, subject to clause 11 and applicable retention law. The Client should use available self-service controls where appropriate. Reasonable fees for additional assistance may apply under clause 5.6; no fee shall excuse or delay a mandatory obligation.

8 Subcontracting Relationships (Subcontractors)

8.1 The Client grants general written authorization for the Subcontractors identified in Annex ./8.10. Before an additional or replacement Subcontractor engaged directly by the Contractor begins processing the Client’s personal data, the Contractor shall provide at least thirty (30) calendar days’ advance email notice identifying the provider, processing activities and locations, intended commencement date and applicable international-transfer safeguards. The Client may object during that period on reasonable data protection grounds. The parties shall work in good faith to resolve the objection, including through an alternative provider, configuration or safeguards. The proposed Subcontractor shall not process the Client’s personal data while a timely objection remains unresolved. The Contractor shall maintain a dated list consistent with Annex ./8.10; publication alone does not replace email notice. The Client shall maintain a current notification email address. Changes to further processors engaged by a Subcontractor are governed by Clause 8.4. If a timely objection cannot be resolved within 30 days, either party may terminate only the affected service on written notice before the objected-to processing begins. The Contractor shall refund prepaid fees for the unused terminated period. Unaffected services continue; no additional termination compensation is due except where required by law or for an existing breach.

8.2 The Contractor shall obtain the information and audit rights required by Article 28(4) GDPR from its Subcontractors and exercise them as reasonably needed to assist the Client. Requests shall be coordinated through the Contractor and may be met by independent reports and other adequate evidence. This clause does not grant unrestricted direct access to a Subcontractor's facilities or systems or limit mandatory audit rights or supervisory powers.

8.3 The responsibilities of the Contractor and the subcontractor shall be clearly demarcated.

8.4 A Subcontractor may engage further processors subject to equivalent data protection obligations and applicable international-transfer safeguards. The Contractor shall promptly forward notice of an additional or replacement further processor to the Client by email after receiving notice from the relevant Subcontractor. The notice shall identify the further processor, processing activities and locations, applicable transfer safeguards, intended effective date and the upstream notice and objection periods, to the extent available. The thirty-day advance period in Clause 8.1 does not apply to these downstream changes. The Client may object on reasonable data protection grounds within the period stated in the notice. The Contractor shall provide a reasonable opportunity to object; if the upstream timetable does not permit this before the change, affected processing shall be suspended until that opportunity has been provided. The parties shall work in good faith to resolve objections. If a timely objection remains unresolved when the change takes effect, the Contractor shall suspend affected processing or provide an agreed alternative that avoids the objected-to further processor. Suspension shall continue until the objection is resolved or such an alternative is in place. The Contractor remains responsible for its Subcontractors' data protection obligations in accordance with Article 28(4) GDPR and Clause 8.9. If no compliant alternative is agreed within 30 days, either party may terminate only the affected service under the refund and continuity provisions of clause 8.1.

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 Before allowing a Subcontractor to process the Client's personal data, the Contractor shall assess its suitability and enter into a binding agreement imposing the data protection obligations required by Article 28(4) GDPR. Relevant compliance information shall be made available on reasonable request, subject to confidentiality and the safeguards in clause 6.8.

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 review Subcontractor compliance on a risk-based basis and at least annually, using independent assurance reports, questionnaires or other appropriate evidence. It shall retain relevant records for the period required to demonstrate compliance and provide necessary information under clause 6.8.

8.9 Where a Subcontractor fails to fulfil its data protection obligations under this Agreement, the Contractor shall be liable to the Client for the damage caused by such failure to the same extent as for its own conduct, in accordance with Art. 28(4) GDPR. Any such liability shall be subject to the liability provisions of Clause 12. The liability provisions of this section (8.9.) shall be without prejudice to the mandatory provisions of Articles 28 and 82 of the General Data Protection Regulation (GDPR).

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 A Subcontractor is a provider processing the Client's personal data on the Contractor's behalf. Providers processing solely as independent controllers, and providers with no access to such personal data, are not Subcontractors for those activities. A service is not excluded merely because it is ancillary. The Contractor remains responsible for correctly classifying and protecting the processing.

9 Obligations to notify

9.1 The Contractor shall notify the Client without undue delay after becoming aware of a personal data breach affecting personal data processed on the Client's behalf. Notice shall be sent to the Client's designated notification email or, if none is current, its administrative account contact. The Contractor may provide information in phases as it becomes available without undue further delay. A notice is not an admission of fault or liability. To the extent available, it shall include:

(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 The Contractor shall notify the Client without undue delay of material failures to comply with this DPA that affect the Client's personal data. Unsuccessful attempts that do not compromise that data do not by themselves constitute a personal data breach; the Contractor shall assess security events and escalate them where required by clause 9.1 or applicable law.

9.3 To the extent legally permitted, the Contractor shall inform the Client without undue delay of supervisory inspections or legally binding measures materially relating to the Client's personal data. This does not require disclosure of legally privileged information or information whose disclosure is prohibited by law.

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's instructions shall relate to the agreed processing and be consistent with this DPA and applicable law. Instructions requiring new functionality, a material scope change or migration are subject to clause 4.2, without limiting mandatory data protection obligations.

10.2 Instructions may be given by the Client's authorized account administrators and the contacts designated in Annex 10.2. The Contractor may reasonably verify authority before acting on an instruction.

10.3 Instructions may be documented in the service configuration or sent by email to the designated contacts. Oral instructions must be confirmed in writing before implementation, except where immediate action is required by applicable law.

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 At the Client's choice, the Contractor shall return the personal data through the available export functionality or another reasonably agreed format and delete remaining copies after the end of services, unless applicable law requires retention. The Client shall communicate its choice within 30 days after termination, unless a later date is agreed in writing; absent a choice, deletion shall apply. Active-system deletion shall occur without undue delay. Residual backup copies shall remain protected, isolated from ordinary use and deleted through the normal documented, time-limited backup cycle; if restored for recovery, deletion instructions shall be reapplied. Any legally retained data shall be limited to the required purpose and period. Bespoke export or migration work may be charged at reasonable rates agreed in advance, without limiting mandatory return or deletion duties.

11.2 The Contractor shall require its Subcontractors to return or delete the Client's personal data consistently with clause 11.1 and their applicable legal obligations. It shall obtain reasonable verification, which may include contractual attestations and provider records, and make a written confirmation available on request.

11.3 On reasonable request, the Contractor shall confirm completion of deletion, identifying any remaining restricted backup copies or legally retained data and their applicable retention basis. This does not require disclosure of other customers' information or unrestricted access to provider media.

11.4 The Contractor may retain records necessary to demonstrate lawful processing, comply with legal obligations or establish, exercise or defend legal claims, only for as long as reasonably necessary or legally required. Retained records remain confidential and shall not be used to continue providing the terminated service.

12 Liability

12.1 Each party is responsible for its own obligations under applicable data protection law. Mandatory liability towards data subjects, including joint and several liability and recourse under Article 82 GDPR where applicable, is unaffected. The allocation below governs contractual claims between the parties only to the extent permitted by law.

12.2 Subject to clause 12.5, the Contractor's aggregate contractual liability under or in connection with this DPA shall not exceed the fees paid or payable by the Client for the affected services during the twelve months preceding the event giving rise to the claim. If the services have been provided for less than twelve months, the cap is the fees paid or payable for that shorter period. A liability cap expressly agreed for data protection claims in a separately negotiated written agreement prevails. Amounts recovered for the same loss under the service agreement and this DPA shall not be recovered twice.

12.3 Subject to clause 12.5, the Contractor shall not be liable for indirect or consequential loss or loss of profits, revenue, business opportunity or goodwill. Each party shall take reasonable steps to mitigate loss. These exclusions do not excuse performance of the Contractor's processing, security or assistance obligations.

12.4 To the extent permitted by law, the Client shall indemnify the Contractor against third-party claims and reasonable defense costs to the extent caused by the Client's unlawful instructions, unlawful submission of personal data or breach of its obligations under clause 4. The indemnity does not cover loss caused by the Contractor's own breach or relieve it of the duty to identify and refuse unlawful instructions. The Contractor shall promptly notify the Client of the claim, allow reasonable control of the defense and provide reasonable cooperation. No settlement admitting liability or imposing non-monetary obligations on the Contractor may be made without its consent, not to be unreasonably withheld.

12.5 The limitations, exclusions and indemnity in clauses 12.2 to 12.4 do not restrict liability for fraud, wilful misconduct, gross negligence, death or personal injury, or any liability that cannot lawfully be limited. They do not prejudice mandatory rights, obligations, remedies or burdens of proof under Articles 28 and 82 GDPR, supervisory authority powers, or liability and remedies under applicable Standard Contractual Clauses or mandatory UK transfer instruments. Those mandatory provisions prevail in case of conflict.

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

The competent courts at the Contractor's registered office in Austria shall have exclusive jurisdiction over contractual disputes between the parties, unless a separately negotiated written agreement provides otherwise. This does not restrict data subjects' rights, supervisory authority powers or any mandatory jurisdiction under applicable data protection law or Standard Contractual Clauses.

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 Amendments require agreement in writing, including electronic acceptance where permitted by the service agreement and applicable law. This edition does not retroactively vary an executed customer agreement merely by being published. Individually negotiated terms remain effective until validly amended.

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

Place, date	Place, date
_____	_____
Client represented by [Authorized representative]	Contractor represented by Lukas Böhler as Chief Executive Officer

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

Specific technical and organizational measures

Hosting

The Client chooses EU or US residency at signup or in the applicable order. EU infrastructure is hosted by DigitalOcean in Frankfurt, Germany; US infrastructure is hosted by DigitalOcean in its NYC3 data center in New York, United States. Customer databases, uploaded files and backups are stored within the selected region. The EU production MongoDB database uses DigitalOcean Managed Databases. Logical isolation and the other measures in this Annex apply to both regions. Processing by separate provider services is described in Annex 8.10 and remains subject to clause 5.9.

Encryption

Data transmitted between customer users, Gleap SDKs and Gleap infrastructure is encrypted using TLS 1.2 or higher. Customer databases, backups and uploaded files are encrypted at rest.

Staff authentication and access review

Multi-factor authentication is required for all systems and applications used by Gleap personnel. Staff access permissions are reviewed quarterly. Personal devices are prohibited. Work from home is permitted only through the Contractor’s VPN using company-managed devices, in accordance with Clause 6.6.

Database backups and restoration

Production database backups remain within the Client's selected region. For the EU production MongoDB database, DigitalOcean creates daily backups retained for a rolling seven-day period; full restoration is tested every six months. US-specific retention and restoration arrangements are documented separately and available on request; this clause does not represent a verified US testing frequency. Backup retention does not determine retention of uploaded files, logs or other records. The Contractor shall maintain appropriate recoverability measures in both regions under Article 32 GDPR.

Independent assurance

Gleap is SOC 2 Type II audited for the Security trust services category. The report issued on August 27, 2026 covers April 1 to June 30, 2026 and is available under confidentiality on request. The report defines the systems and period examined; it is not a guarantee that subsequently introduced infrastructure or regions were included, or a warranty of uninterrupted certification. Contractual security obligations remain those in this DPA.

The following general measures also apply

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 contact

The Contractor's contact for privacy questions, instructions and incident reporting is:

Lukas Böhler

privacy@gleap.io

Managing Director, Gleap GmbH

This is an operational contact designation. Where a data protection officer is required or appointed under Articles 37 to 39 GDPR, the Contractor shall provide that officer's contact details and preserve the required independence and absence of conflicting duties.

Annex ./8.10 – Approved Subcontractors

Optional AI and configuration

AI features are optional. The Client's administrators can disable individual AI features. Account-level AI availability is additionally governed by credit availability or, for legacy plans, the AI usage setting. Stopping credit purchases does not immediately stop processing while credits remain or automatic recharge is active. The Client may select among the models offered for configurable AI features. Enterprise plans support bring-your-own-model arrangements, with the endpoint, provider and processing scope defined for the applicable configuration.

Processing scope

Enabled AI features may process messages, tickets, contact details, attachments, prompts, voice recordings, knowledge-base content and connected repository content to the extent needed for the configured features. Processing may include automated background tasks as well as user-initiated requests. Model selection alone does not establish the provider for every supporting operation or the processing region.

Locations and downstream processing

EU accounts use EU AI endpoints and US accounts use US AI endpoints. The OpenAI, Grok and Kai Voice regional endpoint entries below follow that account configuration. This describes the configured endpoints, not every provider operation, supporting service, remote access or onward transfer. Other provider disclosures remain applicable: Anthropic may process in the US or EU; OpenRouter may use downstream hosts in the EU, US or China; and a direct DeepSeek fallback involves China. Any such processing must comply with the Client's documented instructions, clause 5.9 and the required safeguards. Region-restricted arrangements must also address supporting operations and fallbacks. The Contractor shall not enable a route incompatible with an expressly agreed restriction.

Processing instructions and safeguards

The Contractor shall not use the Client's personal data to train AI models or authorize providers to use it for that purpose. The providers below are engaged only for the applicable services. Listing a provider does not remove the requirements of Clauses 5.9 and 8.7 for international transfers or establish that every provider is used for every Client. Changes are subject to Clauses 8.1 and 8.4. The Client may contact the Contractor to agree account-specific restrictions.

Provider	Entity and location	Processing purpose
DigitalOcean	DigitalOcean, LLC 101 Avenue of the Americas, 10th Floor, New York 10013, USA Regional hosting: Frankfurt, Germany (EU) or NYC3, New York, United States (US), according to the selected region	Primary cloud provider: application servers, screenshot rendering and production MongoDB through DigitalOcean Managed Databases.
Postmark	AC PM, LLC 1 N Dearborn Street, Suite 500, Chicago, IL 60602 Server location: USA	Transactional email delivery.

Provider	Entity and location	Processing purpose
OpenAI	OpenAI Ireland Ltd 1st Floor, The Liffey Trust Centre, 117 –126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland Model serving: EU endpoints for EU accounts; US endpoints for US accounts	Optional AI model processing. Other provider processing and onward transfers are subject to the applicable provider agreement and transfer safeguards.
Cloudflare	Cloudflare, Inc. 101 Townsend St., San Francisco, California 94107, USA Uploaded-file storage: selected EU or US region. Global delivery and video-call processing: worldwide	Regional storage and delivery of uploaded screenshots and attachments; video-call infrastructure. Global delivery and calls may involve processing outside the storage region.
Google	Google Ireland Limited Gordon House, Barrow Street Dublin 4, D04 E5W5 Ireland Server location: USA / EU	Optional AI model processing through the Gemini API.
Stripe	Stripe Payments Europe, Limited / Stripe Technology Europe, Limited Ireland Potential future provider; not currently used	Potential future payment provider for customer billing. Not currently processing data for Gleap. Any activation remains subject to the applicable contractual authorization and notification requirements.
Firebase	Google Ireland Limited Gordon House, Barrow Street Dublin 4. Irland	Push notification provider (this feature must be manually activated)
Paddle	Paddle.com Market Ltd. Judd House. 18-29 Mora Street. London, EC1V 8BT	Payment provider (customer billing)
Grok / xAI	SpaceXAI LLC 1450 Page Mill Road, Palo Alto, California, USA privacy+enterprise@x.ai Model serving: EU endpoints for EU accounts; US endpoints for US accounts	Optional AI model processing. Other provider processing and onward transfers are subject to the applicable provider agreement and transfer safeguards.
Anthropic	Anthropic Ireland, Limited Ireland Processing: US or EU; EU-only processing is not guaranteed	Optional AI model processing.
OpenRouter	OpenRouter, Inc. 169 Madison Ave #2404, New York, NY 10016, USA Downstream processing: EU, US or China	Optional AI routing gateway for models including DeepSeek, Qwen, Kimi, MiniMax and GLM. Requests are forwarded to downstream model-hosting providers. Model selection does not guarantee the host or region; full downstream routing control is not currently available.

Provider	Entity and location	Processing purpose
New Relic	New Relic, Inc. 188 Spear Street, Suite 1000, San Francisco, CA 94105, USA Processing: EU, Frankfurt, Germany	Application performance monitoring and logging. Telemetry may include request metadata.
Composio	Sampark Inc. d/b/a Composio 2 Bryant St., Suite 220, San Francisco, CA 94105, USA	Integration platform powering custom-agent tool connections (third-party app actions and triggers configured by the customer).
Mistral AI	Mistral AI SAS 15 rue des Halles, 75001 Paris, France Server location: EU	Optional AI model processing for Mistral models.
Voyage AI (MongoDB)	MongoDB, Inc. 1633 Broadway, 38th Floor, New York, NY 10019, United States Server location: USA	Voyage AI embedding and reranking through MongoDB Atlas for knowledge-base content, tickets and messages used in AI search and retrieval. Atlas is used for AI inference, not production database hosting.
E2B	FoundryLabs, Inc. San Francisco, CA, United States Server location: USA	Isolated cloud sandboxes in which Kai Code works on repositories connected by the customer. Used only when Kai Code is enabled.
Firecrawl	SideGuide Technologies, Inc. (d/b/a Firecrawl) San Francisco, CA, United States Server location: USA	Crawling of customer websites for knowledge-base ingestion and web retrieval for AI agents. Used only for AI features.
TinyFish	TinyFish, Inc. Palo Alto, CA, United States Server location: USA	Web search and page retrieval for AI agents. Used only for AI features.
Datalab	Endless Labs, Inc. (d/b/a Datalab) New York, NY, United States Server location: USA	Conversion of uploaded documents (PDFs, spreadsheets) into machine-readable text for AI processing. Used only for AI features.
DeepSeek	Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. China Privacy contact: privacy@deepseek.com	Direct API fallback for DeepSeek models, primarily served via OpenRouter. Direct processing takes place in China. The account-specific scope and restrictions must be established before relying on provider exclusion.
ElevenLabs	Eleven Labs Inc. USA Kai Voice speech processing: EU endpoints for EU accounts; US endpoints for US accounts	Speech processing for the optional Kai Voice feature, including speech recognition and speech generation. Other provider processing and onward transfers are governed by the applicable provider agreement and transfer safeguards.

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

Client contacts

The Client may designate the following contacts when executing this DPA, through account settings or by email. Until a separate designation is received, authorized account administrators may issue instructions and the administrative account email is the default notification address. The Client shall keep these details current.

Authorized to issue instructions

Name and role: _____
Email: _____
Deputy name and email: _____

Client breach and subprocessor notices

Name and role: _____
Notification email: _____
Deputy email: _____

Contractor authorized to receive instructions

Lukas Böhler, Gleap GmbH
Email: lukas@gleap.io

Contractor breach contact

Lukas Böhler, Gleap GmbH
Email: privacy@gleap.io

Changes

Each party shall notify the other in writing of changes to its contacts. The Client shall keep its notification email address current.

Annex CCPA California service provider terms

Where the California Consumer Privacy Act, as amended (CCPA), applies and the Client is a business, the Contractor acts as a service provider or contractor for the specific business purposes described in clauses 2 and 3. It shall not sell or share that personal information, retain, use or disclose it outside the direct business relationship or for purposes other than those specified in this DPA, or combine it with personal information from other clients or its own consumer interactions, except as expressly permitted by the CCPA and its regulations. The Contractor shall comply with applicable CCPA obligations and provide the same level of privacy protection required of the Client for that processing. It certifies that it understands and will comply with these restrictions. The Contractor shall notify the Client if it determines that it can no longer meet those obligations. The Client may take reasonable and appropriate steps to verify compliant use, stop and remediate unauthorized use, and require assistance with consumer requests. Clauses 5.6, 6.8 and 8 govern assistance, monitoring and further processors without limiting these mandatory rights. Further processors shall be bound by equivalent applicable restrictions. Statutory CCPA meanings apply to terms used in this paragraph.

Attachment./2.1. - Terms of service

The service agreement and applicable order govern the subscribed services. Current standard terms: https://www.gleap.io/legal/terms-of-service