Mantiq Data Processing Agreement

Version 0.1 | October 5, 2026

This agreement governs how Mantiq processes personal data on behalf of the business customer when providing the translation service. Together with its annexes, it forms part of the Agreement with the customer and aligns with Mantiq's Terms and Conditions and Privacy Policy.

1 Parties and Definitions

1.1 The parties are Mantiq Ltd., established in Cambodia, and the business Customer accepting this agreement via its Account Administrator. The identity of the Customer and the authorized Account Administrator is evidenced by the Account's contract records.

1.2 Capitalized terms have the meaning set forth in the Terms and Conditions. Personal data means information relating to an identified or identifiable natural person. Processing includes, among other things, receiving, storing, analyzing, translating, modifying, accessing, disclosing, and deleting.

1.3 Customer Personal Data means personal data that Mantiq processes on behalf of the Customer in Input, Output, analyses, Translation Memories, Terminology, text excerpts retained for quality control, and related job data. A Personal Data Incident means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to such data.

1.4 Applicable Data Protection Law means the data protection law applicable to the relevant processing and the party concerned. This may include the GDPR, UK data protection legislation, or other applicable law. This agreement does not itself determine the territorial applicability of any law.

2 Scope and Roles

2.1 The Customer determines the purpose of the processing, which documents are submitted, who receives access, and how the Output is used. Mantiq processes Customer Personal Data on behalf of the Customer in accordance with this agreement and documented instructions.

2.2 Where the Customer acts as a data controller, Mantiq acts as a data processor. Where the Customer itself acts as a data processor for a client, Mantiq acts as a Subprocessor. The Customer then confirms that it is authorized to engage Mantiq and the Subprocessors listed in Annex 3 and to apply these instructions and terms on behalf of its client.

2.3 A Customer acting as a processor ensures that its instructions align with those of the ultimate data controller. It forwards relevant requests, restrictions, and notifications in a timely manner. Mantiq assists the Customer so that the Customer can assist its client. Direct contact with that client takes place on the Customer's instructions or where required by applicable law or applicable transfer terms.

2.4 The Privacy Policy governs data that Mantiq lawfully processes as a data controller for its own account management, security, administration, communications, and support purposes. A copy of customer content in a support message remains subject to this DPA to the extent that Mantiq processes that content on behalf of the Customer. Storing content in another system does not automatically alter the data protection role.

3 Documented Instructions

3.1 The instructions consist of this agreement and its annexes, the applicable Terms and Conditions, uploads and choices made by Authorized Users in the Service, and additional written instructions that fall within the scope of the agreed Service. The Customer hereby instructs Mantiq to carry out the processing described in Annex 1, including the limited quality logging under Article 5.

3.2 Mantiq processes Customer Personal Data to deliver, secure, support, and monitor the Service and to correct errors in it, in accordance with these instructions. International processing is governed by Article 10. Mantiq does not use the data for its own advertising, the sale of data, or any independent purpose outside the agreed processing.

3.3 Mantiq informs the Customer immediately if, in Mantiq's opinion, an instruction infringes Applicable Data Protection Law. Mantiq may suspend the relevant processing until a lawful instruction or solution becomes available.

3.4 Where Mantiq is legally required to process data beyond the instructions or to disclose data, Mantiq informs the Customer in advance, unless the law prohibits doing so. Mantiq limits the processing to what the legal obligation requires. For international transfers, the applicable rules on government requests and conflicting laws also apply.

3.5 Any instruction that substantially expands the Service or requires special technical measures is assessed separately. The parties may agree in advance on feasibility, the time frame, and costs. This does not limit Mantiq's legal obligations.

4 Obligations of the Customer

4.1 The Customer ensures that there is a valid legal basis, that the required information is provided to data subjects, and that it has the rights and authority required for the Input to be processed. Before uploading, it assesses whether the Service is suitable for the data concerned, the purpose, and the applicable legal requirements.

4.2 The Customer removes or pseudonymizes personal data and sensitive information that are not necessary for the Job. Pseudonymization and segmentation do not automatically render data anonymous. The Customer manages its users, access rights, and login credentials, and reports suspected unauthorized access immediately.

4.3 For special categories of personal data, personal data relating to criminal convictions and offenses, and other regulated information, the Customer verifies the additional legal basis and safeguards. The Service is not designed for state secrets or processing that requires specialized or formally certified environments.

4.4 The Customer's obligations do not limit Mantiq's own obligations regarding security, confidentiality, lawful processing, and incidents.

5 Quality Logging and Data Use

5.1 During the five processing stages, Mantiq may record where corrections were necessary. The log contains adjusted target text fragments and the associated source fragments. It does not contain a complete copy of each translation as a single searchable document. Logging may take place without the Customer having submitted a complaint.

5.2 The log serves to investigate shortcomings in process stages and to make targeted improvements to the software, instructions, and translation workflow within the agreed quality assurance framework. Mantiq limits the fragments to what is necessary for that purpose and retains them for a maximum of ninety days, subject to Article 11.5.

5.3 Access to the quality log is restricted to authorized personnel within quality management. Mantiq does not provide customer content, Translation Memories, or Terminology to other Customers and does not use them in their Jobs. General insights may lead to improvements for other Customers provided those insights do not identify the Customer and do not disclose customer content.

5.4 Mantiq does not use Input, Output, analyses, Translation Memories, Terminology, or text excerpts retained for quality control to train external, underlying, or generative AI models. Mantiq uses vendor products and contractual arrangements that support this restriction for the processing concerned.

6 Confidentiality and Access

6.1 Mantiq handles Customer Personal Data and other confidential customer content in accordance with Section 13 of the Terms and Conditions. Persons who process data are bound by a contractual or applicable statutory obligation of confidentiality and act in accordance with access rules and instructions from Mantiq.

6.2 Internal access to customer content is limited to authorized owners and quality staff to the extent that such access is necessary for quality control, support, security, or complaint handling. Text excerpts retained for quality control are subject to the stricter access restrictions set forth in Article 5.3. Other employees do not have general access to customer channels.

6.3 Currently, quality staff work directly for Mantiq. A freelancer engaged in the future may work under Mantiq's direct authority if appropriate instructions, confidentiality obligations, and access restrictions apply. If the freelancer acts as a separate data processor, the subprocessor requirements of Article 8 must be met in advance. The actual activities determine the role.

6.4 Mantiq limits access to what is necessary, revokes access as soon as it is no longer required, and maintains records of relevant access grants and security events. Worldwide access is subject to Article 10.

7 Security

7.1 Mantiq implements appropriate technical and organizational measures, taking into account the nature of the data, the processing purposes, available technology, implementation costs, and the risks to data subjects. Annex 2 describes the measures and the technical implementation to be confirmed.

7.2 Mantiq reviews the measures periodically and upon relevant changes or incidents. Mantiq may adjust measures provided that the level of protection is not materially reduced as a result. Where processing requires additional measures that the Service cannot provide, the parties shall discuss restricting or suspending such processing.

7.3 No provision guarantees the complete absence of security incidents. Mantiq remains responsible for implementing the agreed and legally required measures.

8 Subprocessors

8.1 The Customer grants general written authorization for the engagement of Subprocessors in accordance with the current Subprocessor List made available to it. The initial list is set out in Annex 3. Where the

Customer is itself a data processor, it confirms that the required authorization from its client has been obtained.

8.2 Mantiq enters into a written agreement with each Subprocessor containing appropriate obligations regarding confidentiality, security, and data protection. For outsourced processing, Mantiq imposes on the Subprocessor substantially the same applicable data protection obligations as those imposed under this DPA. Mantiq remains responsible to the Customer for the performance of those obligations by the Subprocessor.

8.3 Mantiq shall notify the Account Administrator in writing in advance of the addition or replacement of a Subprocessor, providing information on identity, function, locations, and relevant safeguards. The standard notice period is at least thirty days. The Customer shall be given a genuine opportunity to object before the new Subprocessor processes its data.

8.4 The Customer may submit a reasoned objection within that period based on a material risk to data protection or confidentiality. Mantiq shall explore a reasonable technical or contractual solution. If no viable solution exists, the affected use may be terminated before the change takes effect. Credits are governed by the Terms and Conditions, subject to mandatory law or overriding transfer provisions.

8.5 An urgent change does not confer an unrestricted right to bypass the required authorization and prior notification. If applicable law or applicable transfer provisions do not yet permit the change, Mantiq shall restrict or suspend the affected processing until those conditions are fulfilled.

8.6 Upon request, Mantiq shall provide information enabling the Customer to assess the subprocessing arrangements. Where a copy must be provided under a contract or by law, Mantiq may redact trade secrets and irrelevant information, provided that verification of the relevant obligations remains possible.

9 Incidents and Support

9.1 Mantiq notifies the affected Customer without undue delay after Mantiq becomes aware of a Personal Data Incident. The initial notification contains the information available. Mantiq does not delay reporting until the full investigation has been completed.

9.2 The notification is addressed to the Account Administrator via the registered business email address. If necessary, Mantiq also uses a secure channel. To the extent known, the notification includes the nature and timeline of the incident, the data and individuals affected with estimated numbers, the likely consequences, measures taken or proposed, and a point of contact. Mantiq provides any missing information without undue delay.

9.3 Mantiq investigates the incident, takes appropriate measures to stop it and mitigate its consequences, and documents relevant facts and measures. Mantiq assists the Customer with its assessment and any notifications to supervisory authorities or data subjects. A notification or assistance does not constitute an admission of liability.

9.4 The Customer or its client decides on any required external notifications, unless Mantiq is itself subject to a statutory reporting obligation. Where the Customer is a data processor, it forwards the notification in a timely manner to the ultimate data controller.

9.5 Mantiq forwards to the Customer without undue delay any data subject requests regarding Customer Personal Data that Mantiq receives directly and handles the substance of those requests in accordance with the Customer's instructions, unless applicable law requires otherwise. Taking into account the processing and available information, Mantiq assists with access, rectification, erasure, restriction, objection, and data portability.

9.6 Where necessary, Mantiq assists the Customer with security obligations, data protection impact assessments, and prior consultation with a supervisory authority. The parties tailor the information and implementation to the processing concerned and the statutory deadlines.

9.7 For extensive additional assistance, the parties may agree on reasonable costs in advance. Cost agreements shall not prevent timely compliance with statutory obligations. Work required to remedy a breach attributable to Mantiq is not charged to the Customer as additional assistance.

10 Locations and International Processing

10.1 The central server environment is located in Germany. At each phase, OpenAI and Google process the segments and analyses required for that phase. Their legal entities, products, locations, and safeguards are confirmed in Annex 3. Segmentation does not qualify as anonymization.

10.2 Authorized owners and quality staff may be granted worldwide access for the agreed activities. This does not constitute unrestricted authorization for processing in every country. Prior to access, Mantiq assesses whether the location, security, and any required transfer safeguards permit access. If this cannot be ensured, access from that location is restricted or blocked.

10.3 Where Applicable Data Protection Law requires a transfer mechanism, the parties shall implement a valid mechanism prior to such transfer. Annex 4 sets out which supplementary terms are required. Mantiq assists with the required assessment and implements supplementary measures where necessary. A server located in Germany does not eliminate the need to assess access from abroad or further processing.

10.4 The parties handle onward transfers, government requests, and changes in the level of protection in accordance with applicable law and the applicable transfer terms. Where lawful continuation is not possible, they shall restrict or suspend the processing concerned and handle the data in accordance with those terms.

11 Retention, Return, and Deletion

11.1 Source and target documents, analyses, job details, and text excerpts retained for quality control are retained for a maximum of ninety days, unless deleted earlier. The retention period and exceptions are described in further detail in Annex 1. Translation Memories and Terminology remain available until the deletion of the data, the relevant Channel, the associated user, or the Account.

11.2 After deletion, data is no longer available in the active environment. A backup copy may persist for up to twenty-four hours. During this period, protection continues to apply. Mantiq prevents deleted data from becoming available again through recovery. Article 11.5 applies to statutory exceptions.

11.3 Upon termination of processing, the Customer may choose either return followed by deletion, or deletion. The Customer may download available translated documents, Translation Memories, and Terminology beforehand. For other Customer Personal Data covered by a valid return request, Mantiq provides an appropriate secure method of return. The lack of a standard export feature does not limit that obligation.

11.4 The Customer shall communicate its choice prior to Account closure. Upon Account closure without a return request, the closure serves as an instruction to delete active documents, Channels, and language data. Upon request, Mantiq confirms the completed deletion and any lawful exceptions. This DPA continues to apply for as long as Mantiq retains Customer Personal Data.

11.5 In the event of an ongoing complaint, privacy request, incident, or dispute, Mantiq may retain data reasonably necessary to address the matter and preserve evidence, provided a lawful basis exists. Mandatory

statutory retention is subject to the applicable rules. Mantiq restricts access to and use of the data to that purpose and deletes the data as soon as retention is no longer justified. This provision does not derogate from mandatory deletion rules or applicable standard contractual clauses.

11.6 Mantiq ensures that retention and deletion by subprocessors align with the agreed processing. Any vendor setting with a different retention period must be assessed prior to use and, where necessary, addressed in the contract documentation. Mantiq's own deletion periods do not constitute proof of vendors' actual retention periods.

12 Information and Audits

12.1 Mantiq makes available the information necessary to demonstrate compliance with this DPA and cooperates with appropriate audits conducted by the Customer or an independent expert on the Customer's behalf. Mantiq maintains the required records of processing activities and cooperates with competent supervisory authorities.

12.2 Where appropriate, the parties shall first use existing documentation and written inquiries. If that is insufficient, Mantiq facilitates an additional audit or inspection. The parties shall coordinate scope, timing, confidentiality, and security. An audit must not reveal data of other customers or result in unauthorized access to systems.

12.3 Regular audits require reasonable advance notice. In the event of an incident, indications of non-compliance, or a request from a competent supervisory authority, arrangements will be adapted to the urgency. No restriction applies that would impede the exercise of a statutory or contractual right of audit.

12.4 The parties shall agree in advance on reasonable costs for additional audits. Costs shall not prevent a mandatory audit. Mantiq bears the costs of remedying its own defaults. Irrelevant trade secrets may be redacted, provided that compliance can still be effectively assessed.

13 Term, Order of Precedence, and Liability

13.1 This DPA takes effect upon electronic acceptance by the authorized Account Administrator and activation of the Account, as provided in the Terms and Conditions. Mantiq retains a record of the accepted version, date, time, and the relevant Account. The annexes form an integral part of this DPA.

13.2 For the processing of personal data on behalf of the Customer, this DPA takes precedence over the Terms and Conditions. Mandatory law and applicable standard contractual clauses take precedence over conflicting provisions of this DPA and the Terms and Conditions. The Privacy Policy does not unilaterally modify the instructions or protection under this DPA.

13.3 Amendments are handled in accordance with Section 22 of the Terms and Conditions and, for Subprocessors, Article 8 of this DPA. Continued use does not substitute for any additional consent or formality required by applicable law or transfer terms.

13.4 Liability is governed by the Terms and Conditions to the extent lawful and compatible with this DPA and overriding transfer terms. This does not limit mandatory rights of data subjects, powers of supervisory authorities, or obligations that cannot be excluded under applicable law.

13.5 The governing law and dispute resolution provisions of the Terms and Conditions apply to the extent compatible with mandatory law and the provisions on governing law, competent courts, and third-party rights set out in applicable transfer terms.

13.6 Privacy questions and instructions shall be directed to privacy@mantiq.com. For incidents, use the published security contact address: [confirm]. Formal notices are served in accordance with the Terms and Conditions. The final English DPA shall be the legally binding version; this Dutch text is intended for preparation and review.

Annex 1 Description of the Processing

This annex describes the standard processing operations. The content of the specific Job determines which data and persons are actually involved. When processing on behalf of a client, the Customer ensures that this description aligns with that client's instructions.

Component	Description
Subject matter	Automated business translation and text processing of customer documents, including language data and a limited quality log.
Duration and frequency	For each Job and through repeated use of the Service. Retention according to the schedule below; reuse of language data within the relevant Channel.
Operations	Receiving, segmenting, storing, analyzing, translating, reviewing, editing, proofreading, consulting, correcting, returning, and deleting.
Purposes	Performance of Jobs, retention of terminology, reuse, security, support, complaint handling, and quality assurance under Article 5.
Categories of data subjects	Persons named in the Input, including employees, customers, contact persons, vendors, patients, or other individuals, depending on the Job.
Ordinary personal data	For example, names, contact details, job titles, identifying document details, and substantive information about individuals, to the extent provided.
Sensitive data	Special categories of personal data and personal data relating to criminal convictions and offenses may appear in documents. Processing requires the assessment and safeguards set out in Article 4.3; uploading does not constitute certification or a guarantee of suitability.

Processing stages and vendors

Every Job undergoes Analysis, Translation, Review, and Refinement. Analysis uses the source text; Translation uses the source text and analysis; Review uses source text, target text, and analysis; Editing and Proofreading use target text and analysis. Each Job is processed through both OpenAI and Google. The exact allocation of products and phases will be confirmed prior to publication.

For each phase, Mantiq transmits the required text segments and relevant analysis. Mantiq does not transmit the customer name, account name, internal job number, internal task identifier, or file name as separate metadata to the AI provider. Such identifying information may, however, be present within the text itself. Segmenting text limits context and does not anonymize personal data.

Documents, translations, Translation Memories, and Terminology are used within the respective Channel. Channels do not automatically exchange this data. Data from one Customer is not used as language data for another Customer.

Retention periods

Data	Period
Source text, target text, analyses, and job data	Maximum 90 days, unless deleted earlier.
Text excerpts retained for quality control, including the corresponding source excerpts	Maximum 90 days, except where lawful retention is necessary under Article 11.5.
Translation Memories and Terminology	Until the data, Channel, associated user, or Account is deleted.
Backup after deletion	Maximum 24 hours, subject to an applicable statutory exception.
Material for pending matters	For as long as lawfully necessary under Article 11.5; delete thereafter.
Data held by third-party providers	To be confirmed per product prior to publication. Deviations from the other retention periods must be resolved pursuant to Article 11.6.

Annex 2 Technical and Organizational Measures

Mantiq implements measures appropriate to the described processing and risks. The specification below constitutes the security annex to be confirmed. A statement designated as REVIEW does not constitute a representation that the measure has already been technically implemented.

Separation and access control

Mantiq separates Customers and Channels, assigns access rights by role, and restricts internal access pursuant to Article 6. Individuals are instructed and bound by confidentiality obligations. Access is revoked when the work ends. Text excerpts retained for quality control are subject to separate, restricted access.

Authentication and connections

Mantiq uses secure network connections and appropriate credential protection. The Privacy Policy mentions two-factor authentication for administrators and users. The definitive implementation and internal access security must be confirmed prior to publication.

Retention, backups, and recovery

Mantiq configures storage and deletion pursuant to Article 11. Backups persist for a maximum of twenty-four hours following deletion. Upon restoration, prior deletion instructions are reapplied. Appropriate measures protect the availability of personal data and support its recovery in the event of a technical or physical incident.

Logging, maintenance, and incidents

Mantiq maintains relevant security, error, and access logs, restricts access to such logs, and organizes incident investigation and response. Mantiq periodically evaluates the effectiveness of the measures and applies appropriate security updates.

Global internal access

Access from another country is assessed in advance under Article 10. Mantiq limits access to the necessary data and to authorized personnel and secures the devices and connections used. Where safeguards are insufficient, access is restricted or blocked.

Annex 3 Subprocessor List

Working draft of the initial list. Final details of the legal entities, products, locations, retention periods, and contractual safeguards must be available before acceptance by customers. A brand name does not fully identify the contracting party.

Provider	Function	To be confirmed
Hosting provider [name missing]	Hosting of the central environment in Germany.	Legal entity, service, server and backup locations, access from other countries, DPA, and retention periods.
OpenAI [confirm entity]	AI processing in one or more phases.	Contracting party, API product, phases, locations, retention, training settings, and transfer safeguards.
Google [confirm entity]	AI processing in one or more phases.	Contracting party, product, phases, locations, retention, training settings, and transfer safeguards.

Owners and directly associated quality staff under the authority of Mantiq are not listed here as separate Subprocessors. For future freelancers, the role will be evaluated in advance under Article 6.3. A payment provider is included as a Subprocessor to the extent that it actually processes Customer Personal Data on behalf of Mantiq; any independent role it may have in relation to payments is described separately in the Privacy Policy.

Annex 4 Conditional International Transfer Terms

This annex sets out what must be finalized prior to a regulated international transfer. It does not yet incorporate the full official standard contractual clauses and does not constitute an independent transfer mechanism in this working draft.

Identifying transfers and access

Map out at least the chain from Customer to Mantiq in Cambodia, hosting in Germany, processing by AI providers, and internal access from other countries. For each step, determine exporter, importer, data protection role, data involved, locations, and applicable rules. Global access is assessed on the basis of actual countries and circumstances.

Requirements for EEA data

Where EU standard contractual clauses serve as the applicable mechanism, the valid official clauses incorporating the appropriate module and fully completed annexes become part of the Agreement. Module 2 may be appropriate where a data controller acts as exporter and Mantiq as data processor; Module 3 may be appropriate where a data processor acts as exporter and Mantiq as subprocessor. Suitability for the specific transfer must be confirmed, including the territorial applicability of the GDPR to the importer.

The details include the parties and contact persons, a description of the transfer, sensitive data and supplementary safeguards, the competent supervisory authority, security measures, approved subprocessors, relevant elections, and the parties' own choices of governing law and forum. The required transfer impact assessment regarding third-country legislation and practice, as well as any supplementary measures, must also be finalized. The parties shall not modify the official clauses in a manner that prejudices their validity.

Requirements for other jurisdictions

For UK or other regulated transfers, the applicable supplementary official terms or another valid mechanism shall be determined. An EU module shall not be deemed sufficient for every jurisdiction without assessment.

Entry into Effect and Precedence

The final transfer terms apply to the extent legally required and applicable. They shall be validly entered into before the transfer concerned takes place. In the event of any conflict, they shall take precedence pursuant to Article 13.2. If no lawful mechanism is available, the affected processing or access shall not take place.