DATA PROCESSING AGREEMENT

(AVV / Data Processing Addendum – DPA)

for the use of Thalassa Assistant

Version 1.4 – 9 October 2026

This document is designed as an agreement capable of being concluded electronically pursuant to Article 28 GDPR. It applies exclusively to B2B uses in which the customer is the controller and Thalassa Consulting Kft. is the processor. For Thalassa's own processing of personal data (e.g. account, billing, security and contract data), the privacy policy as amended from time to time shall apply.

1. Contracting Parties

Processor	Thalassa Consulting Kft.
Registered office	1188 Budapest, Dozsa György ut 37, Hungary
Product	Thalassa Assistant
Data protection contact	Patrik Talasi
Commercial register / tax data	HU23892543

Controller / Customer	[Company name]
Registered office / address	[Address]
Register data	[Register data]
Authorised representative	[Name / function]
Data protection contact	[E-mail]
Main Agreement / customer account	[Contract / account ID]

This Data Processing Agreement ("DPA") supplements the agreement existing between the parties on the use of Thalassa Assistant ("Main Agreement"). To the extent that provisions of the Main Agreement and of this DPA conflict with regard to the processing of personal data, this DPA shall prevail.

2. Definitions and Scope of Application

2.1 The terms "personal data", "processing", "controller", "processor", "sub-processor", "data subject" and "personal data breach" shall have the meaning given in Regulation (EU) 2016/679 ("GDPR").

2.2 This DPA applies to the extent that Thalassa Consulting Kft. processes personal data on behalf of the customer and in accordance with the customer's documented instructions. It applies in particular to meeting content, voice data, transient transcripts, screen recordings, document extracts retrieved from a local knowledge base, and calendar, contact, e-mail and document data from systems the user has connected to Thalassa (Microsoft 365, Google, providers with an MCP interface), to the extent that these are processed in order to provide the agreed functions.

2.3 To the extent that Thalassa processes personal data for its own purposes and under its own responsibility (in particular contract administration, invoicing, payment processing, fraud prevention, IT security, support metadata and statutory retention obligations), Thalassa acts as an independent controller. Such processing operations do not fall under this DPA.

2.4 This DPA is not the B2C data protection notice and replaces neither the privacy policy for end users nor the customer's obligation to inform meeting participants and other data subjects in accordance with the applicable data protection laws.

3. Subject Matter, Purpose, Nature and Duration of the Processing

3.1 The subject matter of the processing is the technical provision of Thalassa Assistant as an AI-supported real-time meeting assistant with, in particular, the following functions: microphone and system audio processing, speech-to-text transcription, AI-supported answer generation during meetings, local document/PDF knowledge base with retrieval-augmented generation (RAG), processing of manually triggered screenshots, and the creation of meeting briefings and debriefings.

3.2 The processing serves exclusively the provision, securing and technical support of the functions commissioned by the customer. Customer data shall not be used for advertising, profiling for third-party purposes, the sale of data, or the training of the processor's own or third-party generative AI models.

3.3 The processing shall in principle last for the term of the Main Agreement. Content data from meetings shall be processed only transiently, unless otherwise stipulated in Annex 1. Upon termination of the Main Agreement, the deletion and return rules of this DPA shall apply.

4. Instructions of the Controller

4.1 Thalassa shall process personal data exclusively on documented instructions from the customer, including with regard to transfers to third countries, unless Thalassa is required to process by mandatory Union law or applicable national law.

4.2 The Main Agreement, the product configuration activated by the customer, this DPA and lawful written individual instructions constitute the documented instructions of the customer.

4.3 If Thalassa considers an instruction to infringe data protection law, Thalassa shall inform the customer without undue delay and may suspend the execution of the instruction concerned until the matter is clarified.

4.4 The customer remains responsible for the lawfulness of the instructions, the permissibility of the processing and the fulfilment of its information and legal-basis obligations.

5. Obligations of Thalassa as Processor

Processing exclusively within the scope of the customer's documented instructions;

commitment of all persons authorised to process to confidentiality;

implementation of appropriate technical and organisational measures pursuant to Article 32 GDPR;

support of the customer with regard to data subject rights, data protection impact assessments, consultations with supervisory authorities and security incidents, to the extent that the processing by Thalassa is concerned;

maintenance of the legally required records of processing activities as processor;

provision of appropriate evidence of compliance with this DPA;

no use of customer data for model training or product training, unless the customer has previously issued an express, separate and revocable instruction; by default no such training takes place.

6. Confidentiality and Access Restriction

6.1 Access to the customer's personal data shall be granted only to such employees and contractors who require it in order to provide the contractual services. Access rights shall be granted in accordance with the need-to-know and least-privilege principles.

6.2 Persons with access to customer data shall be bound to confidentiality or be subject to a corresponding statutory duty of secrecy.

6.3 Content data shall not be used for general internal analyses unless anonymisation within the meaning of data protection law has been carried out. A mere replacement of names by identifiers (e.g. “User 1”) constitutes pseudonymisation and shall continue to be protected as personal data.

7. Technical and Organisational Measures (TOMs)

7.1 Thalassa shall take appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing. The minimum measures envisaged at the time of conclusion of the contract are described in Annex 2.

7.2 Thalassa may further develop the TOMs, provided that the agreed level of protection is not materially reduced.

7.3 Content data must not be logged in general application, debug or telemetry logs, unless this has been expressly initiated by the customer for the error analysis of a specific support case. Such exceptional cases shall be limited to the necessary minimum and deleted promptly.

8. Sub-processors

8.1 The customer grants Thalassa a general written authorisation to engage the sub-processors listed in Annex 3.

8.2 Thalassa shall inform the customer at least 30 days before the planned engagement of a new sub-processor or the replacement of an existing sub-processor, to the extent that the new service provider processes the customer’s personal data. The information may be provided by e-mail or via a permanently accessible sub-processor update channel.

8.3 The customer may object within this period on comprehensible data protection grounds. If the parties cannot find an appropriate solution, the customer may terminate the specific function concerned or, if this is not technically possible, the Main Agreement in accordance with the rules provided for therein.

8.4 Thalassa shall contractually oblige each sub-processor to data protection obligations that correspond to the material requirements of this DPA, and shall remain responsible to the customer for that sub-processor’s performance under data protection law.

9. Processing in the EU / EEA and Third-Country Transfers

9.1 The productive Thalassa infrastructure for meeting content data shall in principle be aligned with European AWS regions. For Amazon Bedrock, an EU geographic or a single EU region shall be used; global inference profiles must not be used as the standard configuration for customer data under this DPA. An exception to this applies to the extent that the user requests the web search and the AI answer generation required for this takes place via the direct API of Anthropic PBC; audio data and the ongoing transcript are not covered by this exception.

9.2 For speech-to-text, the Deepgram EU endpoint shall be used, to the extent that it supports the required function. An automatic fallback to a non-European speech-to-text endpoint is not permitted for customer data under this DPA unless an appropriate third-country transfer basis has previously been established and the customer has been informed accordingly.

9.3 To the extent that a sub-processor is established in a third country or can lawfully access personal data from a third country, Thalassa shall ensure a legal basis pursuant to Chapter V GDPR before the processing begins. To the extent that no adequacy decision applies, the standard contractual clauses of the European Commission pursuant to Implementing Decision (EU) 2021/914 shall in particular be used in the relevant module constellation and, where necessary, additional measures shall be implemented.

9.4 For Deepgram, Inc. as a US sub-processor, a DPA including appropriate standard contractual clauses shall be concluded. In addition, the use of customer data for model improvement, benchmarking or comparable secondary purposes shall be deactivated contractually and technically.

9.5 For Anthropic PBC as a US sub-processor, processing via the direct API is approved exclusively for the web search requested by the user. The Anthropic data processing agreement, including the standard contractual clauses incorporated therein, which forms part of the contract pursuant to the Commercial Terms of Service applicable to the service, shall apply for this purpose. The use of the transmitted customer data for model training or comparable model improvement purposes shall be excluded. Only the content required for this function pursuant to Annex 1 shall be transmitted; audio data and the ongoing transcript shall not be transmitted to Anthropic PBC.

9.6 Where an AI model is provided via Amazon Bedrock, the processing on behalf of Thalassa takes place via AWS. To the extent that AWS, according to its respective product configuration, does not pass inputs and outputs on to the model provider, the model provider shall not be treated as a recipient of customer data solely because of the provision of the model. The direct API call to Anthropic PBC for the web search requested by the user is approved in accordance with clause 9.5 and Annex 3. If, in addition, the direct API of a further model provider is used, that provider must be included in Annex 3 before productive use and an appropriate DPA/transfer mechanism must be established.

10. Support with Data Subject Rights

10.1 Thalassa shall support the customer, taking into account the nature of the processing and insofar as technically possible, by appropriate measures in fulfilling requests for access, rectification, erasure, restriction, data portability and objection.

10.2 If a data subject request is received directly by Thalassa and concerns data that Thalassa processes exclusively on behalf of a customer, Thalassa shall in principle forward the request to the customer concerned and shall not answer it independently, unless there is a statutory obligation to handle it directly.

11. Personal Data Breaches

11.1 Thalassa shall inform the customer of a personal data breach falling under this DPA without undue delay after becoming aware of it and in principle within 24 hours, to the extent that sufficient information is available at that time.

11.2 The notification shall contain, to the extent available, a description of the nature of the incident, the categories of data and groups of persons concerned, the likely consequences, the countermeasures already taken or planned, as well as a contact point for further enquiries.

11.3 The notification does not constitute an acknowledgement of a breach of duty. Thalassa shall document relevant security incidents and shall support the customer with statutory notification and communication obligations.

12. Data Protection Impact Assessment and Consultation of the Authority

To the extent that the processing by Thalassa is relevant for a data protection impact assessment of the customer, Thalassa shall make available to the customer the technical and organisational information reasonably available and shall support the customer to an appropriate extent. The same shall apply to any prior consultation of the competent supervisory authority that may be required.

13. Return and Deletion

13.1 After the end of the provision of the processing services, Thalassa shall, at the customer's choice, delete or return personal data, to the extent that it has not already been deleted automatically under the product design and no statutory retention obligation precludes this.

13.2 Meeting audio, transient transcripts, screenshots and generated meeting content shall not be stored as a permanent meeting record in the Thalassa cloud. Technically unavoidable volatile processing or buffer copies shall be removed automatically after completion of the respective processing operation; content data shall not form part of permanent logs.

13.3 Knowledge bases stored locally by the customer, local transcripts, exports or locally stored debriefings lie outside the cloud deletion carried out by Thalassa and shall be managed by the customer on its end devices.

14. Evidence and Audit Rights

14.1 Thalassa shall make available to the customer, upon request, the information reasonably required to demonstrate compliance with this DPA. Existing independent audit reports, certifications and security documentation may be used as evidence on a priority basis.

14.2 The customer may carry out an audit, or have an audit carried out by an independent auditor bound to secrecy, where there are concrete indications of a material non-conformity or where legally required. Audits shall be carried out with reasonable prior notice, during usual business hours and in such a way that the operations, security and confidentiality of other customers are not impaired.

14.3 To the extent that an audit arises exclusively from a special scope requested by the customer and no material breach of duty by Thalassa is established, reasonable additional costs may be charged to the customer following prior agreement.

15. Special Categories of Data, Meeting Participants and Minors

15.1 The service is not designed to collect special categories of personal data in a targeted manner. However, such data may be processed incidentally due to the open content of meetings, screenshots or document extracts. The customer shall ensure that a permissible legal basis or exception pursuant to Article 9 GDPR or other applicable law exists for this purpose.

15.2 The customer is responsible for informing meeting participants and other data subjects, in the respectively required form, about the use of speech-to-text and AI functions and, to the extent necessary, for obtaining effective consents or other legal bases.

15.3 Thalassa does not create voiceprints, does not carry out biometric speaker identification for the unique identification of a person, and uses the meeting audio data exclusively for speech-to-text, unless another function is expressly agreed.

15.4 In normal meeting operation, Thalassa does not assess the personality, emotions, employee performance, examination performance or aptitude of a person. To the extent that a separate practice mode offers objective feedback on answers, it must not be designed as an automated decision with legal or similarly significant effect.

15.5 In the case of minors, it is incumbent on the customer to comply with the respectively applicable age, consent and information obligations. This DPA does not create any entitlement to the independent B2C registration of children.

16. Further Applicable Data Protection Laws

16.1 To the extent that further data protection laws apply to the processing in addition to the GDPR, the parties shall be obliged to comply with them within the scope of their respective roles. These may include in particular the UK GDPR and the Data Protection Act 2018, the Swiss Data Protection Act, US state data

protection laws (including the CCPA/CPRA, to the extent applicable), and Canadian, Australian, Japanese, Korean and Singaporean data protection provisions.

16.2 To the extent that the law of a jurisdiction provides for additional mandatory processor/service provider obligations, these shall apply in addition. For restricted transfers from the United Kingdom or Switzerland, the respectively required transfer instruments or adaptations shall be used.

16.3 For the purposes of the CCPA/CPRA, to the extent applicable, Thalassa processes personal information only for the contractually specified business purposes, does not sell or share it for cross-context advertising, and does not combine it with personal information from other sources unless this is legally permissible and necessary for the provision of the service.

16.4 The regional supplements in Annexes 4A to 4C apply automatically to the extent that the respective data protection law is applicable to the customer, the data subjects, the processing or an international data transfer. To the extent that a regional supplement contains mandatory stricter requirements, it shall prevail over the general provisions of this DPA for the matter concerned.

17. Liability, Term and Termination

17.1 The liability of the parties shall be governed by the mandatory statutory provisions and, to the extent permissible, by the liability provisions of the Main Agreement. No provision of this DPA limits the rights of data subjects or the powers of authorities.

17.2 This DPA enters into force upon acceptance and applies for as long as Thalassa processes personal data on behalf of the customer.

17.3 If the Main Agreement ends, this DPA shall end upon completion of all deletion, return and evidence obligations required under data protection law.

18. Order of Precedence, Applicable Law and Amendments

18.1 In the event of conflicts between this DPA and the Main Agreement, this DPA shall take precedence with regard to data protection and processing on behalf of a controller. Mandatory standard contractual clauses or other mandatory transfer instruments shall prevail over conflicting provisions of this DPA.

18.2 To the extent that the Main Agreement does not contain another effective choice of law, Hungarian law shall apply, subject to the precedence of directly applicable Union law. Mandatory data protection provisions and the competences of the supervisory authorities remain unaffected.

18.3 Amendments to this DPA require text form or another electronically documented form. Purely technical updates to the annexes, in particular security measures or sub-processor lists, may be made in accordance with the amendment and information procedure described in this DPA, provided that the level of protection is not materially reduced.

19. Electronic Conclusion

19.1 The parties agree that this DPA may be concluded electronically. Electronic acceptance may take place in particular by means of an electronic signature or by a clearly logged click-to-accept procedure.

19.2 The electronic conclusion record shall contain at least the identity or the customer account, the company name, the name and function of the acting person, the confirmed authority of representation, the e-mail address, the date and time of acceptance, the accepted document version, as well as tamper-proof evidence of the accepted version.

19.3 After acceptance, the customer shall receive a durable copy of the DPA or a permanently available download link to the specific version accepted. Thalassa shall retain the evidence of the conclusion of the contract in accordance with the statutory and contractual requirements.

Annex 1 – Description of the Processing

Feature	Description
Subject matter	Provision of Thalassa Assistant as a real-time meeting assistant.
Purpose	Speech-to-text, context-related AI answer generation, RAG from the local knowledge base, screenshot analysis, briefing/debriefing, retrieval of calendar, contact, e-mail and document data from systems connected by the user for briefings and answers, as well as – to the extent requested by the user – AI answer generation with web search via Anthropic PBC and technically necessary provision of the service.
Duration	Term of the Main Agreement; meeting content data in principle only transient during the respective processing.
Data subjects	Users of the customer; employees; applicants; meeting participants; customers, prospects, advisers, legal/financial contacts and other persons whose data appears in meeting content, screenshots, document extracts, or in calendar entries, contacts, e-mails and documents of connected systems.
Categories of data	Audio/voice data; conversation content; transient transcripts; names/contact details, to the extent contained in the content; screenshots; selected document extracts; calendar entries, contact data, e-mail content and document extracts from connected systems; encrypted access credentials (OAuth tokens) for those systems; technical session and request metadata; generated answers; where applicable special categories of data, if introduced by the customer or meeting participant.
Processing operations	Capturing/streaming, transmitting, speech-to-text, pseudonymising/minimising, temporary buffering, retrieval, retrieval from connected systems, creation of e-mail drafts on the user's instruction, AI inference, user-requested web search, displaying, generating, technically necessary caching and deletion.
Voice biometrics	No voiceprints and no biometric speaker identification for unique identification.
Profiling / assessment	No regular assessment of personality, emotion, employee performance, examination performance or aptitude; no automated decision-making with legal or similarly significant effect as a standard function.

A. Data Flow and Storage Logic

Microphone/system audio is captured locally and transmitted to Deepgram for speech-to-text. For productive EU use, the Deepgram EU endpoint shall be used.

The transcript generated is processed only transiently for the ongoing session or request. It is not stored permanently as a complete meeting record in the Thalassa cloud.

Customer documents/PDFs and the local knowledge base remain in principle on the end device. For the AI answer, however, selected text extracts and context passages determined by local retrieval may be transmitted to the AI processing. Therefore, it must not be claimed that all document content never leaves the end device without exception.

Screenshots are transmitted and processed only where the function is activated/manually triggered and only for the respective request.

To the extent that the user requests the web search, the request intended for the AI answer is processed via the direct API of Anthropic PBC. In this process, the user's question, the user's preparation details and the document extracts selected from the local knowledge base by retrieval are transmitted. Audio data and the ongoing transcript are not transmitted to Anthropic PBC in this process; the speech-to-text processing remains with the Deepgram EU endpoint.

Generated answers and debriefings are not stored centrally as a complete meeting history, unless an expressly agreed function provides for this. The user may store or export results locally.

Connections to Microsoft 365, Google and providers with an MCP interface are set up voluntarily by the user, who can disconnect them at any time; for business accounts, prior consent by the customer's administrator may be required. Only what a specific preparation or an ongoing conversation needs is retrieved. Calendar, contact and e-mail content passes transiently through the backend in Frankfurt and is not stored there; file content from OneDrive, SharePoint and Google Drive is processed by the app on the end device and discarded after the conversation, on a change of account and on disconnection. For the AI answer, the same path applies as for document extracts from the local knowledge base. The content is not used for training and is not added to the knowledge base. Thalassa does not send e-mails; on the user's instruction it merely creates a draft in the user's mailbox. Thalassa does not access Gmail.

The access credentials issued by Microsoft or Google after consent are stored by Thalassa encrypted with AES-256-GCM in the backend in Frankfurt, bound to the account and the provider. On disconnection they are deleted and a Google credential is additionally revoked with Google; on deletion of the account they are deleted together with all other account data. Data from Google interfaces is subject to the Google API Services User Data Policy, including the Limited Use requirements.

The desktop app connects directly to the server configured by the customer for providers with an MCP interface; the credentials for this remain with the customer. Retrieved text is indexed and searched on the end device; selected extracts follow the existing request path for answers and briefings. Each tool call takes place only after confirmation by the user.

Account, billing and general usage metadata may be stored separately as data under Thalassa's own responsibility; they do not automatically fall under this Annex.

B. Retention

Category of data	Cloud retention	Rule
Raw audio	No permanent storage by Thalassa	Streaming processing; the Deepgram contract/configuration must exclude secondary use and storage that is not necessary.
Transcript	No permanent storage	Transient during session/request; automatic deletion after the end of processing.
Screenshots	No permanent storage	Transient per request; automatic deletion after processing.
RAG document extracts	No permanent content repository as a document archive	Only for inference; no training use.
Generated answers	No permanent meeting record	Only transient, unless the user stores/exports locally.
Technical logs	Metadata only to the extent necessary	No meeting content in standard logs; retention periods in accordance with the security/operations concept.
Calendar, contacts, e-mails of connected systems	No permanent storage	Transient per preparation/request via the backend; automatic deletion after processing.
File content of connected systems	No storage in the cloud	Processed on the end device; discarded after the conversation, on a change of account and on disconnection.
Access credentials (OAuth tokens)	Encrypted (AES-256-GCM), Frankfurt	Until disconnection (deletion, for Google additionally revocation) or until deletion of the account.

Category of data	Cloud retention	Rule
Source references of a preparation	Metadata only (file name, link, version, time of retrieval)	No content; lifetime as the user's associated briefing.

Annex 2 – Technical and Organisational Measures (TOMs)

1. Access Control

Role- and permission-based access in accordance with the least-privilege principle.

MFA for privileged administration accesses.

Regular review and withdrawal of access rights that are no longer needed.

No disclosure of productive access credentials; secrets held in appropriate secret management systems.

2. Transmission Security

Encryption of data in transit using current TLS procedures (at least TLS 1.2, to the extent technically supported).

Preferred use of private AWS network paths/PrivateLink for internal cloud communication, to the extent technically appropriate.

No unencrypted transmission of meeting content data over public networks.

3. Encryption of Stored Data

Cloud metadata and other persistent personal data are stored in encrypted form, to the extent that the respective AWS service supports this.

Key management via AWS KMS or equivalent procedures; access to keys according to least privilege.

Meeting content data shall not be stored persistently; this additionally reduces the attack surface.

Access credentials for connected systems (OAuth tokens) are encrypted with AES-256-GCM before being stored in the database; the ciphertext is bound to the account and the provider, so that a value copied from the database cannot be used against another account. Access rights are requested according to the principle of least privilege; no right to send e-mails is requested.

4. Data Minimisation and Pseudonymisation

Transmission to AI services only of the context required for the specific answer.

Removal or replacement of directly identifying information, to the extent that this is possible without loss of functionality.

Pseudonymised data continues to be treated as personal data.

No training use of customer data.

5. Logging and Monitoring

Security and operational logs do not, as far as possible, record meeting content.

Monitoring for availability, unauthorised access and security-relevant anomalies.

Administrative changes and security-relevant events are logged in a traceable manner.

6. Tenant Separation

Logical separation of customer/user data by unique tenant/user assignment and access controls.

No intentional intermingling of meeting content of different customers.

Testing of the authorisation and tenant boundaries before productive releases.

7. Secure Development

Code review and controlled release processes for production-relevant changes.

Dependency and vulnerability management with prompt remediation of critical security vulnerabilities.

Separation of development, test and production environments, to the extent that personal production data is concerned.

No use of real customer data in development/testing, unless strictly necessary and separately secured.

8. Availability and Recovery

Appropriate backup and recovery procedures for persistent operational and account data.

Restart and incident response procedures for essential systems.

Due to the transient processing, meeting content data is in principle not envisaged as part of the backup inventory.

9. Incident Response

Documented process for the detection, assessment, containment and remediation of security incidents.

Internal escalation paths and responsibilities.

Process for customer notification pursuant to Section 11 of this DPA.

10. Supplier Control

DPA/data processing agreement with sub-processors prior to productive processing of the customer's personal data.

Review of the transfer mechanisms for third-country providers.

Deepgram: use the EU endpoint; conclude DPA/SCCs; deactivate use for model improvement/benchmarking.

Amazon Bedrock: use EU region or EU geo inference; no global inference as standard for customer data.

Annex 3 – Approved Sub-processors

Provider / registered office / role	Purpose	Place of processing	Transfer mechanism / particularity
Amazon Web Services (AWS) AWS group / relevant contracting entity Cloud sub-processor	Hosting, authentication, backend/database services and Amazon Bedrock AI inference	EU regions; primarily Frankfurt. Bedrock only in-region or EU geo for customer data.	AWS DPA; relevant transfer mechanisms for third-country access. Bedrock inputs/outputs must not be passed on to model providers.
Deepgram, Inc. (USA) Sub-processor	Real-time speech-to-text	EU-hosted endpoint for productive use	Deepgram DPA + SCCs (Module 3, to the extent relevant); no model improvement; no benchmarking; no non-EU fallback without prior compliance review.
Anthropic PBC (USA) Sub-processor	AI answer generation with web search, to the extent requested by the user	USA	Anthropic DPA including standard contractual clauses, as part of the Commercial Terms of Service; no use of the inputs for model training.
DeepL SE (Cologne, Germany)	Live translation, to the extent requested by the	as per the DeepL agreement	DeepL data processing agreement (DeepL API Pro); no use of the inputs

Provider / registered office / role	Purpose	Place of processing	Transfer mechanism / particularity
Sub-processor	user		for model training; third-country transfers only in accordance with Chapter V GDPR (DeepL DPA including standard contractual clauses).

Note: A direct call to a model provider is approved only for the providers and purposes expressly listed in this Annex. Anthropic PBC is included for the web search requested by the user, subject to the above conditions. Any further direct API provider must be included in this Annex before productive use and the required DPA/third-country transfer review must be completed.

Microsoft, Google and providers with an MCP interface are not sub-processors of Thalassa. They are providers engaged by the customer itself; Thalassa accesses the data held there only with the user's consent and within the permissions granted by the customer, on a read-only basis or – for e-mail drafts – in the user's mailbox. The contractual relationship with these providers and the legal basis for the processing there remain the customer's responsibility.

Annex 4 – International Data Transfers and Regional Supplements

A. EEA: For transfers from the EEA to a third country, the requirements of Articles 44 et seq. GDPR apply. To the extent necessary, the standard contractual clauses pursuant to Implementing Decision (EU) 2021/914 shall be incorporated in the respectively appropriate module constellation.

B. United Kingdom: To the extent that the UK GDPR applies and a "restricted transfer" is present, the parties shall use the respectively valid UK International Data Transfer Addendum or another permissible transfer instrument.

C. Switzerland: To the extent that the Swiss Data Protection Act is applicable, the EU standard contractual clauses shall, where necessary, be supplemented in such a way that Swiss terms, supervisory authorities and applicable provisions are covered.

D. USA / California: To the extent that the CCPA/CPRA is applicable, Thalassa acts, with regard to the customer data processed on behalf of the customer, as a service provider/contractor to the extent provided for by law and does not use the data outside the contractually specified business purposes.

E. Further states: For Canada, Australia, Japan, the Republic of Korea, Singapore and other target markets, the mandatory local data protection provisions shall apply in addition. This Annex is intended to establish a global minimum standard, but does not replace a mandatory local supplementary agreement if a jurisdiction requires one.

F. Anthropic PBC / user-requested web search: To the extent that the user requests the web search, the user's question, the user's preparation details and the document extracts retrieved from the local knowledge base may be transmitted to Anthropic PBC in the United States. Audio data and the ongoing transcript are not covered by this. The transfer takes place on the basis of the Anthropic DPA including the standard contractual clauses incorporated therein and to the exclusion of any use of the transmitted customer data for model training or comparable model improvement purposes.

Annex 4A – Switzerland (Swiss FADP Addendum)

This Annex applies automatically to the extent that the Swiss Federal Act on Data Protection (DSG/FADP) is applicable to the customer, a data subject, the processing or a disclosure of data abroad.

CH-1. Terms and order of precedence. Terms such as personal data, processing, controller, processor and particularly sensitive personal data shall, within the scope of this Annex, be interpreted in accordance with the Swiss FADP. The general protection obligations of this DPA shall apply in addition. To the extent that the FADP and the GDPR are applicable in parallel, both sets of rules shall be complied with; mandatory statutory requirements remain unaffected.

CH-2. Processing on behalf of a controller. Thalassa processes personal data falling under this DPA only for the documented purposes and instructions of the customer, ensures appropriate data security, confidentiality and sub-processor control, and supports the customer in giving effect to the rights of data subjects under the Swiss FADP.

CH-3. Disclosure of data abroad. A disclosure from Switzerland to a state with an adequate level of data protection may be based on the respective adequacy regime under Swiss law. For disclosures to states without an adequate level of protection, appropriate safeguards pursuant to Article 16 FADP shall be used, in particular standard data protection clauses recognised by the FDPIC or another permissible transfer mechanism.

CH-4. Swiss adaptations of the EU SCCs. To the extent that the standard contractual clauses of the European Commission pursuant to Implementing Decision (EU) 2021/914 are used for a transfer subject to the Swiss FADP, the parties shall in principle choose the GDPR standard of protection for the entire transfer covered. The FDPIC remains competent for compliance with the Swiss FADP; where the GDPR applies in parallel, the statutory competence of the relevant EU supervisory authority continues to exist alongside it.

CH-5. Judicial protection of Swiss data subjects. References in the EU SCCs to a “Member State” must not be interpreted in such a way as to prevent a data subject with habitual residence in Switzerland from asserting the rights to which they are entitled under the SCCs or the Swiss FADP before a court competent under Swiss law at their place of habitual residence.

CH-6. Law applicable to the SCCs. To the extent that the EU SCCs are simultaneously used to fulfil GDPR requirements, the law of an EU Member State effectively chosen therein shall remain decisive for the SCCs. Mandatory rights and competences under the Swiss FADP are not excluded thereby.

CH-7. Switzerland–USA. For transfers to the United States, an adequacy regime existing under Swiss law for recipients effectively certified under the Swiss-U.S. Data Privacy Framework may be used, to the extent that their certification covers the specific type of data and processing. Otherwise, appropriate safeguards, in particular the recognised SCCs with the required Swiss supplements, shall be used.

CH-8. Supervisory authority. The competent Swiss supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC), to the extent that the processing or transfer concerned is subject to the Swiss FADP.

Annex 4B – United Kingdom (UK GDPR Addendum)

This Annex applies automatically to the extent that the UK GDPR, the Data Protection Act 2018 or the UK rules on international data transfers are applicable to the processing.

UK-1. Terms. References in this DPA to the GDPR, personal data, controller, processor, supervisory authority and data subject rights shall, within the scope of this Annex, include the corresponding terms of the UK GDPR and the Data Protection Act 2018.

UK-2. Transfer UK → Thalassa. As long as Hungary or the EEA is fully covered by UK adequacy regulations, a transfer of personal data from a UK customer to Thalassa in Hungary may be based on that adequacy regulation; an IDTA or UK Addendum is in principle not additionally required for this purpose.

UK-3. Restricted transfers without adequacy. To the extent that an international transfer restricted under the UK GDPR is not covered by a UK adequacy regulation, the party responsible for the transfer shall ensure a permissible transfer mechanism before the transfer begins. For this purpose, in particular the respectively valid International Data Transfer Addendum to the EU SCCs approved by the ICO, or the International Data Transfer Agreement (IDTA), may be used.

UK-4. EU SCCs + UK Addendum. If the EU SCCs have already been agreed for the same data flow, the respectively valid ICO Addendum to those EU SCCs shall in principle be used. The mandatory components of the official ICO Addendum are not amended or replaced by this DPA. The parties shall complete the information required therein on the basis of this DPA, its annexes and the specific transfer constellation.

UK-5. Transfer Risk Assessment / Data Protection Test. To the extent that UK law requires a transfer risk assessment or the statutory data protection test where appropriate safeguards are used, the party responsible for this shall carry out that assessment. Thalassa shall make available the reasonably available information on recipients, place of processing, security measures and sub-processors.

UK-6. United States. For a restricted transfer from the United Kingdom to a US recipient, the UK Extension to the EU-U.S. Data Privacy Framework may be used, to the extent that the statutory requirements are met. This requires in particular an effective certification of the recipient for the UK Extension and the category of data concerned. Otherwise, appropriate safeguards shall be used.

UK-7. Supervisory authority. The competent UK data protection supervisory authority is the Information Commissioner's Office (ICO), to the extent that UK data protection law applies to the processing concerned.

UK-8. Further development. If an IDTA or Addendum approved by the ICO is replaced by a new binding version or amended in accordance with the update mechanism provided for, the parties shall use the respectively legally effective version for new or continued transfer mechanisms within the relevant transitional periods.

Annex 4C – United States (U.S. State Privacy Addendum)

This Annex applies automatically to the extent that an applicable comprehensive data protection law of a US state governs the relationship between the customer and Thalassa as business/controller and service provider/contractor/processor. For California, the following CCPA/CPRA provisions apply in particular.

US-1. Roles and terms. To the extent that applicable US data protection law defines terms such as business, controller, service provider, contractor, processor, consumer, personal information, personal data, sensitive data, sale, sharing or targeted advertising, these terms shall have the meaning of the respectively applicable law. The customer acts as business/controller and Thalassa as service provider/contractor/processor, to the extent that the statutory requirements for this are met.

US-2. Specified business purposes. Thalassa processes personal data received on behalf of the customer exclusively for the specifically agreed business purposes: real-time speech-to-text, context-related AI answer generation, RAG from the local knowledge base, screenshot analysis, briefing/debriefing, technical provision of the session, as well as security, troubleshooting and support, to the extent that these activities are necessary for the provision of the service or instructed by the customer.

US-3. No sale or sharing. Thalassa does not sell the customer's personal data and does not "share" it for cross-context behavioral advertising or a comparable statutorily defined advertising purpose. Thalassa receives no consideration for the disclosure of such customer data for its own advertising or data trading purposes.

US-4. Purpose limitation. Thalassa must not retain, use or disclose the customer's personal data for purposes outside those described in US-2 or outside the direct business relationship with the customer, unless applicable law expressly permits this.

US-5. No impermissible combination. Thalassa does not combine personal data received on behalf of the customer with personal data from other customers, from its own end-user relationships or from third-party sources, to the extent that such combination is impermissible for service providers/contractors/processors under applicable US data protection law. Technically necessary security, abuse and integrity checks remain possible only to the extent permitted by law.

US-6. No AI training and no own profiling. The customer's personal data shall not be used for training generative models, for third-party model improvement, personalised advertising, the processor's own aptitude assessments or the processor's own profiling. An automated decision with legal or similarly significant effect concerning a data subject is not a standard function of the processing on behalf of the controller.

US-7. Consumer rights. Thalassa supports the customer to an appropriate extent with applicable consumer rights, in particular information/access, deletion, correction and data portability, as well as with legally relevant opt-out or restriction rights. Thalassa responds to requests from data subjects concerning data processed on behalf of the customer in principle only on the customer's instruction, unless there is a statutory obligation to respond directly.

US-8. Sensitive data. Sensitive personal data is processed only to the extent that it is necessary for the function initiated by the customer. Thalassa does not use sensitive data to infer characteristics of a person outside the commissioned service, and does not use voice data for biometric identification or emotion recognition.

US-9. Sub-processors. Thalassa obliges sub-processors that process the customer's personal data to contractual restrictions that are compatible with the obligations applicable to Thalassa under this Annex. Thalassa remains responsible for the selection and contractual engagement of the sub-processors in accordance with this DPA.

US-10. Control and evidence. The customer may take reasonable and proportionate steps to verify that Thalassa processes the customer's personal data in accordance with this Annex and applicable US data protection law. The evidence and audit provisions in Section 14 of this DPA shall apply with priority for this purpose; further mandatory statutory control rights remain unaffected.

US-11. Notification of inability to comply. If Thalassa determines that it can no longer meet a statutory obligation applicable to this Annex as a service provider, contractor or processor, Thalassa shall inform the customer without undue delay. The customer may demand reasonable steps to stop and remediate impermissible use.

US-12. California CCPA/CPRA. To the extent that the CCPA/CPRA is applicable, the parties confirm that the business purposes described in US-2 constitute the limited and specified purposes of the disclosure. Thalassa undertakes to comply with the statutory restrictions applicable to service providers and contractors, including the prohibition on selling or sharing, the purpose and relationship limitation, the legally required support of the customer, and the obligation to enable the customer to take reasonable verification and remediation measures.

US-13. Certification. Thalassa certifies that it has understood the restrictions laid down in this Annex for service providers/contractors/processors and that it complies with them, to the extent that the respective US data protection law is applicable to the processing.

US-14. Health data / HIPAA. This DPA is not a Business Associate Agreement under HIPAA. Unless a separate written agreement has been expressly concluded, the customer must not configure or market the service as a HIPAA-regulated business associate solution for protected health information.

US-15. Children's and B2C data. This B2B DPA does not replace any consumer-related information, age or consent obligations under COPPA or other US children's and consumer data protection law. To the extent that the customer introduces data of minors into the processing on behalf of the controller, the customer remains responsible for the statutory authority and information required for this; Thalassa processes such data exclusively within the scope of the agreed service.

Legal status of the regional supplements: 08.09.2026. Mandatory statutory changes and the respectively valid official transfer instruments remain decisive.

Annex 5 – Electronic Acceptance / Signature Record

Customer / company	[automatically from account]
Name of the acting person	[Input]
Function / title	[Input]
E-mail	[Input / verified]

Customer / company	[automatically from account]
Authority of representation confirmed	☐ Yes
DPA version	1.4 – 09.10.2026
Time of acceptance	[automatic timestamp]
Document hash / audit ID	[automatically generated]
Electronic acceptance	☐ I accept this DPA on behalf of the customer named above.

Recommended technical evidence: immutable storage of the accepted document version or its hash, audit ID, timestamp, account/customer ID, verified e-mail, and dispatch of a copy to the customer. IP address and device information should only be stored if this is necessary for evidentiary/security purposes and is transparently described in the privacy policy.

Acceptance

By accepting or signing electronically, the acting person confirms that they are authorised to represent the customer and that they are concluding this DPA including its annexes on behalf of the customer.

Annex 6 – OECD Country Supplements to the Master DPA

This Annex supplements the Master DPA for customers with a registered office or relevant data processing in an OECD member state. It is designed as a country annex and does not amend the main text of the Master DPA, unless mandatory national data protection law requires a different rule.

Status of country coverage: 08.09.2026. The 38 OECD member states are covered. Accession candidates and partner states are not covered as long as they are not OECD members.

Activation rule: The section on a country applies automatically if the customer is established there, data subjects are resident there, or the respective national data protection law applies mandatorily to the processing for other reasons.

Order of precedence: In the event of conflicts, mandatory local data protection law shall prevail over this Annex. In all other respects, the Master DPA, the TOMs, the sub-processor rules and the third-country transfer rules shall continue to apply unchanged. For Switzerland, the United Kingdom and the USA, the detailed annexes already present shall remain applicable with priority; the following country sections serve there additionally as an assignment and brief supplement.

No local legal advice: This country annex is a standard contractual extension. It does not replace a local legal review in the case of enterprise customers, regulated industries, health data, employee data, children, education/examination situations or public authority customers.

Country index: Australia; Austria; Belgium; Canada; Chile; Colombia; Costa Rica; Czechia; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Israel; Italy; Japan; Republic of Korea; Latvia; Lithuania; Luxembourg; Mexico; Netherlands; New Zealand; Norway; Poland; Portugal; Slovakia; Slovenia; Spain; Sweden; Switzerland; Türkiye; United Kingdom; United States.

6.1 Uniform OECD Base Clauses

Thalassa processes customer data exclusively for the provision, securing, maintenance and billing of Thalassa Assistant and not for independent advertising, sales, profiling or AI training purposes.

To the extent that a local law uses terms such as processor, service provider, contractor, operator, entrusted processor or comparable roles, Thalassa shall act functionally in that role, to the extent that the customer determines the purposes and means of the processing concerned.

Sub-processors may only be engaged in accordance with the rules of the Master DPA. Thalassa contractually obliges these providers to a materially equivalent level of data protection.

Data subject rights are coordinated via the customer, unless Thalassa is required to act directly under mandatory law.

Data breaches are handled in accordance with the stricter requirements of the Master DPA and of the respectively mandatory local law.

Third-country transfers take place only in accordance with the transfer rules of the Master DPA and of the respectively applicable local provisions.

6.2 EU/EEA OECD States: GDPR Core plus National Supplement

For the following OECD states in the EU/EEA area, the GDPR core of the Master DPA applies as the primary rule for processing on behalf of a controller. The respective national supplement concerns in particular national implementing laws, employee data, professional secrecy obligations, fine/authority competences, telecommunications/cookie rules and sectoral special provisions.

Country	Local supplementary law	Country supplement
Austria	DSG and GDPR implementing provisions	For Austrian customers, national rules apply in addition, in particular on authority competence, data protection secrecy, employee data and special statutory retention/information obligations.
Belgium	Belgian Data Protection Act of 30.07.2018 and GDPR	For Belgian customers, national rules apply in addition, in particular on the supervisory authority, language/information obligations, employee data and criminal/administrative law particularities.
Czechia	Act No. 110/2019 Coll. and GDPR	For Czech customers, national rules apply in addition, in particular on public bodies, employee data, the supervisory authority and special national legal bases.
Denmark	Danish Data Protection Act and GDPR	For Danish customers, national rules apply in addition, in particular on employee data, national ID numbers, the supervisory authority and sectoral special provisions.
Estonia	Personal Data Protection Act and GDPR	For Estonian customers, national rules apply in addition, in particular on the supervisory authority, public bodies, electronic communications and sectoral obligations.
Finland	Data Protection Act 1050/2018 and GDPR	For Finnish customers, national rules apply in addition, in particular on employee data, public registers, the supervisory authority and sector-specific obligations.
France	Loi Informatique et Libertés and GDPR	For French customers, national rules apply in addition, in particular on CNIL requirements, employee data, professional secrecy obligations, health data and cookies.
Germany	BDSG, state data protection acts and GDPR	For German customers, national rules apply in addition, in particular on employee data, data protection officers, persons bound by professional secrecy, state law and supervisory authorities.
Greece	Law 4624/2019 and GDPR	For Greek customers, national rules apply in addition, in particular on the supervisory authority, employee data, public bodies and electronic communications.

Country	Local supplementary law	Country supplement
Hungary	Info Act CXII of 2011 and GDPR	As Thalassa is established in Hungary, Hungarian implementing provisions apply in addition in any event; for Hungarian customers, local NAIH/information obligations apply additionally.
Iceland	Act No. 90/2018 and EEA GDPR	For Icelandic customers, the EEA implementation of the GDPR applies with national supplements on the supervisory authority, employee data and sectoral obligations.
Ireland	Data Protection Act 2018 and GDPR	For Irish customers, national rules apply in addition, in particular on DPC competence, employee data, children, electronic communications and authority requirements.
Italy	Codice Privacy, Legislative Decree 196/2003 as amended, and GDPR	For Italian customers, national rules apply in addition, in particular on Garante requirements, employee data, professional secrecy obligations, health data and marketing/cookies.
Latvia	Personal Data Processing Law and GDPR	For Latvian customers, national rules apply in addition, in particular on the supervisory authority, public bodies, employee data and sector-specific provisions.
Lithuania	Law on Legal Protection of Personal Data and GDPR	For Lithuanian customers, national rules apply in addition, in particular on the supervisory authority, employee data, public bodies and national procedures.
Luxembourg	Act of 01.08.2018 and GDPR	For Luxembourg customers, national rules apply in addition, in particular on CNPD competence, employee data, professional secrecy obligations and the financial/advisory sector.
Netherlands	UAVG and GDPR	For Dutch customers, national rules apply in addition, in particular on AP competence, BSN/national identifiers, employee data and sectoral special provisions.
Norway	Personal Data Act and EEA GDPR	For Norwegian customers, the EEA implementation of the GDPR applies with national supplements on the supervisory authority, employee data and electronic communications.
Poland	Polish Data Protection Act 2018 and GDPR	For Polish customers, national rules apply in addition, in particular on UODO competence, employee data, public bodies and national procedures.
Portugal	Law 58/2019 and GDPR	For Portuguese customers, national rules apply in addition, in particular on CNPD competence, employee data, children, electronic communications and retention.
Slovakia	Act No. 18/2018 Coll. and GDPR	For Slovak customers, national rules apply in addition, in particular on the supervisory authority, employee data, public bodies and national procedures.
Slovenia	ZVOP-2 and GDPR	For Slovenian customers, national rules apply in addition, in particular on the supervisory authority, video/employee data, public bodies and national procedures.
Spain	LOPDGDD and GDPR	For Spanish customers, national rules apply in addition, in particular on AEPD requirements, digital rights, employee data, children and cookies.
Sweden	Data Protection Act 2018:218 and GDPR	For Swedish customers, national rules apply in addition, in particular on IMY competence, employee data, public bodies and sectoral provisions.

6.3 Non-EU / Non-EEA OECD States: Country Supplements

For the following states, additional national data protection obligations are more likely, because the GDPR does not automatically replace the entire local regime of the customer. The clauses apply in addition and only to the applicable extent.

Australia

Local legal basis / classification	Privacy Act 1988, Australian Privacy Principles (APPs) and Notifiable Data Breaches Scheme.
Local classification	The customer remains responsible for transparency, legal basis and APP-compliant use. Thalassa processes on behalf of the customer and not for its own content purposes.
Processor / service provider obligations	Thalassa uses customer data only for the agreed business purposes, implements appropriate security measures and supports the customer with APP-related enquiries.
Transfer / access	To the extent that customer data is transferred from Australia to Europe, the contractual safeguards of the Master DPA apply. The customer remains responsible for its APP 8 assessment.
Data subject rights / security incidents	Thalassa supports access/rectification requests and reports security incidents in accordance with the stricter standard from the Master DPA and local law.
Particularity for Thalassa Assistant	Meeting content, audio, transcripts and screenshots are not used for profiling, advertising or AI training.

Canada

Local legal basis / classification	PIPEDA and applicable provincial private sector laws, in particular Quebec, Alberta and British Columbia, to the extent relevant.
Local classification	The customer remains the accountable organisation/controller in the local sense. Thalassa acts as service provider/processor for the purposes determined by the customer.
Processor / service provider obligations	Thalassa processes data only for the commissioned service, and maintains confidentiality, security measures, deletion and sub-processor control.
Transfer / access	Cross-border processing in Europe must be disclosed to the extent that the customer is obliged to do so under local law. For Quebec data, additional transfer and contractual assessments may be required.
Data subject rights / security incidents	Thalassa supports access/correction requests and security incidents. Notifications are made to the customer in such a way that the customer can meet its own Canadian notification obligations.
Particularity for Thalassa Assistant	For regulated Canadian customers, health data, public bodies or Quebec Law 25 cases, a separate local review should be carried out before an enterprise conclusion.

Chile

Local legal basis / classification	Law No. 19.628; in addition Law No. 21.719 as the reformed data protection regime from the respectively applicable date of entry into force.
Local classification	Until the new provisions enter into force, the existing Chilean provisions remain

Local legal basis / classification	Law No. 19.628; in addition Law No. 21.719 as the reformed data protection regime from the respectively applicable date of entry into force.
	decisive; thereafter the tightened obligations apply in addition.
Processor / service provider obligations	Thalassa processes only within the scope of the customer's instruction, complies with security measures and does not use customer data for its own secondary purposes.
Transfer / access	International transfers take place in accordance with the Master DPA, SCCs or equivalent safeguards, to the extent that local law requires this.
Data subject rights / security incidents	Thalassa supports ARCO/data subject rights and incidents within the scope of what is technically possible.
Particularity for Thalassa Assistant	For Chilean customers, a renewed review of this Annex is required because of the change in the law, as soon as Law No. 21.719 applies in full.

Colombia

Local legal basis / classification	Law 1581 of 2012, Decree 1377 of 2013 and relevant SIC requirements.
Local classification	The customer remains Responsable del Tratamiento; Thalassa acts as Encargado del Tratamiento, to the extent that it processes personal data on behalf of the customer.
Processor / service provider obligations	Thalassa processes only on instruction, maintains confidentiality and takes security measures against unauthorised access, loss, alteration or disclosure.
Transfer / access	Transfers to Europe take place within the framework of the contractual safeguards and, to the extent necessary, on the basis of authorisation, contract or another permissible basis.
Data subject rights / security incidents	Thalassa supports the customer with consulta/reclamo processes and with security incidents.
Particularity for Thalassa Assistant	Customer data is not sold, not used for Thalassa's own AI training and not used outside the direct service.

Costa Rica

Local legal basis / classification	Law No. 8968 on Protection of the Person regarding the Processing of Personal Data and supplementary provisions.
Local classification	The customer remains responsible for consent, information and purpose limitation. Thalassa acts as a service provider on behalf of the customer.
Processor / service provider obligations	Thalassa processes data only in a purpose-bound and confidential manner and with appropriate security measures.
Transfer / access	International processing in Europe takes place in accordance with the contractual rules of the Master DPA and with the requirements of applicable Costa Rican law.
Data subject rights / security incidents	Thalassa supports access, rectification, erasure and objection within the scope of what is technically possible.
Particularity for Thalassa Assistant	For special categories of data or minors, a separate local lawfulness

Local legal basis / classification	Law No. 8968 on Protection of the Person regarding the Processing of Personal Data and supplementary provisions.
	assessment by the customer is required.

Israel

Local legal basis / classification	Protection of Privacy Law, 1981, Protection of Privacy Regulations and applicable Authority guidance.
Local classification	The customer remains database owner/controller in the local sense; Thalassa acts as an outsourcing/processing service provider for the agreed purposes.
Processor / service provider obligations	Thalassa complies with appropriate security, confidentiality and sub-processor obligations and does not process customer data for its own purposes.
Transfer / access	Transfers to Europe take place in accordance with the Master DPA and in compliance with the Israeli rules on data transfers abroad.
Data subject rights / security incidents	Thalassa supports data subject rights and security incidents, to the extent technically possible and contractually required.
Particularity for Thalassa Assistant	For Israeli databases with registration, security level or outsourcing requirements, additional documentation obligations may exist on the customer's side.

Japan

Local legal basis / classification	Act on the Protection of Personal Information (APPI) and requirements of the Personal Information Protection Commission.
Local classification	The customer remains business operator/controller; Thalassa processes as an entrusted service provider for the commissioned purposes.
Processor / service provider obligations	Thalassa does not process data beyond the scope of the entrustment relationship, protects confidentiality and controls sub-processors.
Transfer / access	Transfers between Japan and the EU/EEA may be facilitated by applicable adequacy/transfer mechanisms; additional information or consents remain the customer's responsibility, to the extent necessary.
Data subject rights / security incidents	Thalassa supports disclosure, correction, cessation of use and incident handling under the APPI to the extent technically possible.
Particularity for Thalassa Assistant	AI training, advertising, profiling and changes of purpose using customer data are excluded, unless the customer lawfully instructs otherwise on a separate basis.

Republic of Korea

Local legal basis / classification	Personal Information Protection Act (PIPA) and requirements of the Personal Information Protection Commission.
Local classification	The customer remains personal information controller; Thalassa acts as outsourced processor/consignee within the scope of the customer's instruction.
Processor / service provider	Thalassa maintains purpose limitation, technical and organisational security,

Local legal basis / classification	Personal Information Protection Act (PIPA) and requirements of the Personal Information Protection Commission.
obligations	sub-processor control and confidentiality.
Transfer / access	International transfers to Europe take place in accordance with the Master DPA and the Korean requirements for cross-border processing/outsourcing, to the extent applicable.
Data subject rights / security incidents	Thalassa supports data subject requests and incident notifications with the required information on the nature, scope and measures taken.
Particularity for Thalassa Assistant	For Korean user information, children or sensitive data, separate information/consent obligations are to be reviewed by the customer.

Mexico

Local legal basis / classification	Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP), Regulations and applicable requirements of the authorities.
Local classification	The customer remains Responsable; Thalassa acts as Encargado for the contractually defined purposes.
Processor / service provider obligations	Thalassa processes only on the customer's instruction, maintains confidentiality, implements security measures and does not pass data on to third parties, except to approved sub-processors.
Transfer / access	International processing in Europe takes place on the basis of the Master DPA and the local transfer requirements, to the extent applicable.
Data subject rights / security incidents	Thalassa supports ARCO rights and security incidents to the extent technically possible.
Particularity for Thalassa Assistant	Customer data is not sold, not shared for advertising and not used for Thalassa's own AI models.

New Zealand

Local legal basis / classification	Privacy Act 2020, Information Privacy Principles and Notifiable Privacy Breach regime.
Local classification	The customer remains agency/controller in the local sense. Thalassa acts as a service provider for the commissioned processing.
Processor / service provider obligations	Thalassa uses data only for the provision of the service, protects it appropriately and restricts sub-processors in accordance with the Master DPA.
Transfer / access	Cross-border processing in Europe takes place in accordance with the safeguards of the Master DPA. The customer remains responsible for its IPP 12 assessment.
Data subject rights / security incidents	Thalassa supports access/correction requests and reports relevant privacy breaches to the customer.
Particularity for Thalassa Assistant	Thalassa does not create voiceprints, carry out biometric identification or conduct AI training with customer data.

Switzerland

Local legal basis / classification	Federal Act on Data Protection (DSG/FADP) and the Ordinance on Data Protection.
Local classification	The customer remains the controller within the meaning of the Swiss FADP; Thalassa acts as processor, to the extent that it processes on behalf of the customer.
Processor / service provider obligations	The Swiss supplement already present in the Master DPA remains applicable with priority. This country clause additionally confirms purpose limitation, confidentiality and sub-processor control.
Transfer / access	Transfers to the EU/EEA are in principle regarded as transfers to states with an adequate level of protection. For other third countries, SCCs or equivalent safeguards shall be used.
Data subject rights / security incidents	Thalassa supports rights of access, erasure and rectification as well as security incidents.
Particularity for Thalassa Assistant	For particularly sensitive personal data, high-risk profiling or Swiss professional secrecy obligations, a separate customer review is required.

Türkiye

Local legal basis / classification	Law No. 6698 on the Protection of Personal Data (KVKK) and the relevant decisions/guidelines of the KVKK authority.
Local classification	The customer remains data controller; Thalassa acts as data processor/service provider within the scope of the customer's instruction.
Processor / service provider obligations	Thalassa processes only in a purpose-bound manner, takes security measures, maintains confidentiality and restricts sub-processors.
Transfer / access	International transfers to Europe require the bases provided for by Turkish law, to the extent that the KVKK is applicable.
Data subject rights / security incidents	Thalassa supports data subject rights and security incidents, to the extent technically possible and legally required.
Particularity for Thalassa Assistant	For Turkish customers, additional information, consent, registration or transfer obligations may exist; these are to be reviewed separately before a broad launch.

United Kingdom

Local legal basis / classification	UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations and ICO guidance.
Local classification	The customer remains controller or processor; Thalassa acts as processor or sub-processor in accordance with the actual allocation of roles.
Processor / service provider obligations	The UK supplement already present in the Master DPA remains applicable with priority. This country clause additionally confirms the binding effect of instructions, security, sub-processor control and no AI training.
Transfer / access	UK-to-EEA transfers are in principle facilitated under the respectively applicable

Local legal basis / classification	UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations and ICO guidance.
	UK adequacy rule; otherwise the IDTA or UK Addendum shall be used.
Data subject rights / security incidents	Thalassa supports UK GDPR rights, DPIA/TRA requirements and personal data breaches.
Particularity for Thalassa Assistant	For UK education, employment, financial services or legal customers, a sectoral review should be carried out in the case of enterprise use.

United States

Local legal basis / classification	U.S. state privacy laws, in particular the CCPA/CPRA and other applicable state consumer privacy acts; sectorally in addition, e.g. HIPAA/GLBA/FERPA, only where expressly agreed.
Local classification	The customer remains business/controller. Thalassa acts as service provider, contractor, processor or sub-processor, to the extent that the respective state law provides for this.
Processor / service provider obligations	The USA supplement already present in the Master DPA remains applicable with priority. Customer data is not sold, not shared for cross-context behavioral advertising, not used to train the processor's own AI models and not used outside the direct business relationship.
Transfer / access	Data processing in Europe takes place in accordance with the Master DPA. Access by US sub-processors such as Deepgram is permissible only under a DPA, SCCs/DPF or another permissible transfer basis and with secondary use deactivated.
Data subject rights / security incidents	Thalassa supports consumer requests, security incidents and evidence obligations under the applicable state laws.
Particularity for Thalassa Assistant	HIPAA-, GLBA-, FERPA- or employment-law-regulated US data may only be processed if the required additional contracts and product configurations have been expressly concluded.

6.4 Implementation Checklist for the Website / Signature Flow

At B2B checkout, the country of the customer's establishment must be recorded; IP geolocation alone is not sufficient as a contractual basis.

The customer must confirm whether it acts as controller or as processor for third parties. If processor: Thalassa is sub-processor.

The customer must confirm that the signing person is authorised to represent it.

The accepted Master DPA must be logged with version number, OECD annex, timestamp, account ID and document hash.

For regulated industries, an enterprise flag should be set so that an additional local review is triggered.

For B2C users, this DPA must not be used as a data protection notice. There, terms of service, privacy policy, cookie/tracking notices and rules on minors are required separately.