AUFTRAGSVERARBEITUNGSVEREINBARUNG

(AVV / Data Processing Addendum – DPA)

für die Nutzung von Thalassa Assistant

Version 1.4 – 9. Oktober 2026

Dieses Dokument ist als elektronisch abschließbare Vereinbarung nach Art. 28 DSGVO konzipiert. Es gilt ausschließlich für B2B-Nutzungen, bei denen der Kunde Verantwortlicher und Thalassa Consulting Kft. Auftragsverarbeiter ist. Für eigene Datenverarbeitungen von Thalassa (z. B. Konto-, Abrechnungs-, Sicherheits- und Vertragsdaten) gilt die jeweils aktuelle Datenschutzerklärung.

1. Vertragsparteien

Auftragsverarbeiter	Thalassa Consulting Kft.
Sitz	1188 Budapest, Dozsa György ut 37, Ungarn
Produkt	Thalassa Assistant
Datenschutzkontakt	Patrik Talasi
Handelsregister-/Steuerdaten	HU23892543

Verantwortlicher / Kunde	[Firmenname]
Sitz / Anschrift	[Anschrift]
Registerdaten	[Registerdaten]
Vertretungsberechtigte Person	[Name / Funktion]
Datenschutzkontakt	[E-Mail]
Hauptvertrag / Kundenkonto	[Vertrags-/Account-ID]

Diese Auftragsverarbeitungsvereinbarung („AVV“) ergänzt den zwischen den Parteien bestehenden Vertrag über die Nutzung von Thalassa Assistant („Hauptvertrag“). Soweit Regelungen des Hauptvertrags und dieser AVV hinsichtlich der Verarbeitung personenbezogener Daten widersprüchlich sind, geht diese AVV vor.

2. Begriffe und Anwendungsbereich

2.1 Die Begriffe „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Unterauftragsverarbeiter“, „betroffene Person“ und „Verletzung des Schutzes personenbezogener Daten“ haben die Bedeutung der Verordnung (EU) 2016/679 („DSGVO“).

2.2 Diese AVV findet Anwendung, soweit Thalassa Consulting Kft. personenbezogene Daten im Auftrag des Kunden und nach dessen dokumentierten Weisungen verarbeitet. Sie findet insbesondere auf Meeting-Inhalte, Sprachdaten, transiente Transkripte, Bildschirmaufnahmen, aus einer lokalen Wissensbasis abgerufene Dokumentauszüge sowie Kalender-, Kontakt-, E-Mail- und Dokumentdaten aus Systemen, die der Nutzer selbst mit Thalassa verbunden hat (Microsoft 365, Google, Anbieter mit MCP-Schnittstelle), Anwendung, soweit diese zur Bereitstellung der vereinbarten Funktionen verarbeitet werden.

2.3 Soweit Thalassa personenbezogene Daten für eigene Zwecke und in eigener Verantwortlichkeit verarbeitet (insbesondere Vertragsverwaltung, Rechnungsstellung, Zahlungsabwicklung, Betrugsprävention, IT-Sicherheit, Support-Metadaten und gesetzliche Aufbewahrungspflichten), handelt Thalassa als eigenständiger Verantwortlicher. Diese Verarbeitungen fallen nicht unter diese AVV.

2.4 Diese AVV ist nicht der B2C-Datenschutzhinweis und ersetzt weder die Datenschutzerklärung für Endnutzer noch die Pflicht des Kunden, Meetingteilnehmer und sonstige betroffene Personen nach den anwendbaren Datenschutzgesetzen zu informieren.

3. Gegenstand, Zweck, Art und Dauer der Verarbeitung

3.1 Gegenstand der Verarbeitung ist die technische Bereitstellung von Thalassa Assistant als KI-gestütztem Echtzeit-Meeting-Assistenten mit insbesondere folgenden Funktionen: Mikrofon- und Systemaudioverarbeitung, Speech-to-Text-Transkription, KI-gestützte Antwortgenerierung während Meetings, lokale Dokumenten-/PDF-Wissensbasis mit Retrieval-Augmented Generation (RAG), Verarbeitung manuell ausgelöster Screenshots sowie Erstellung von Meeting-Briefings und Debriefings.

3.2 Die Verarbeitung dient ausschließlich der Erbringung, Sicherung und technischen Unterstützung der vom Kunden beauftragten Funktionen. Kundendaten werden nicht für Werbung, Profilbildung zu fremden Zwecken, Verkauf von Daten oder Training eigener oder fremder generativer KI-Modelle verwendet.

3.3 Die Verarbeitung dauert grundsätzlich für die Laufzeit des Hauptvertrags. Inhaltsdaten aus Meetings werden nur transient verarbeitet, soweit in Anlage 1 nichts Abweichendes festgelegt ist. Nach Beendigung des Hauptvertrags gelten die Lösch- und Rückgaberegeln dieser AVV.

4. Weisungen des Verantwortlichen

4.1 Thalassa verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, einschließlich Weisungen zu Übermittlungen in Drittländer, es sei denn, Thalassa ist aufgrund zwingenden Unionsrechts oder anwendbaren nationalen Rechts zur Verarbeitung verpflichtet.

4.2 Der Hauptvertrag, die vom Kunden aktivierte Produktkonfiguration, diese AVV und rechtmäßige schriftliche Einzelweisungen bilden die dokumentierten Weisungen des Kunden.

4.3 Hält Thalassa eine Weisung für datenschutzrechtswidrig, informiert Thalassa den Kunden unverzüglich und kann die Ausführung der betreffenden Weisung bis zur Klärung aussetzen.

4.4 Der Kunde bleibt für die Rechtmäßigkeit der Weisungen, die Zulässigkeit der Verarbeitung und die Erfüllung seiner Informations- und Rechtsgrundlagenpflichten verantwortlich.

5. Pflichten von Thalassa als Auftragsverarbeiter

Verarbeitung ausschließlich im Rahmen dokumentierter Weisungen des Kunden;

Verpflichtung aller zur Verarbeitung befugten Personen auf Vertraulichkeit;

Umsetzung angemessener technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO;

Unterstützung des Kunden bei Betroffenenrechten, Datenschutz-Folgenabschätzungen, Konsultationen mit Aufsichtsbehörden und Sicherheitsvorfällen, soweit die Verarbeitung durch Thalassa betroffen ist;

Führung der gesetzlich erforderlichen Aufzeichnungen über Verarbeitungstätigkeiten als Auftragsverarbeiter;

Bereitstellung angemessener Nachweise zur Einhaltung dieser AVV;

keine Nutzung von Kundendaten für Modelltraining oder Produkttraining, außer der Kunde erteilt zuvor eine ausdrückliche, gesonderte und widerrufliche Weisung; standardmäßig findet kein solches Training statt.

6. Vertraulichkeit und Zugriffsbeschränkung

6.1 Zugriff auf personenbezogene Kundendaten erhalten nur solche Beschäftigten und Auftragnehmer, die ihn für die Erbringung der vertraglichen Leistungen benötigen. Zugriffsrechte werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben.

6.2 Personen mit Zugriff auf Kundendaten sind zur Vertraulichkeit verpflichtet oder unterliegen einer entsprechenden gesetzlichen Verschwiegenheitspflicht.

6.3 Inhaltsdaten werden nicht für allgemeine interne Analysen verwendet, soweit hierfür keine Anonymisierung im datenschutzrechtlichen Sinn vorliegt. Eine bloße Ersetzung von Namen durch Kennungen (z. B. „User 1“) gilt als Pseudonymisierung und wird weiterhin wie personenbezogene Daten geschützt.

7. Technische und organisatorische Maßnahmen (TOM)

7.1 Thalassa trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses vorgesehenen Mindestmaßnahmen sind in Anlage 2 beschrieben.

7.2 Thalassa darf die TOM weiterentwickeln, sofern das vereinbarte Schutzniveau nicht wesentlich abgesenkt wird.

7.3 Inhaltsdaten dürfen nicht in allgemeinen Anwendungs-, Debug- oder Telemetrie-Logs protokolliert werden, soweit dies nicht für die Fehleranalyse eines konkreten Supportfalls ausdrücklich vom Kunden veranlasst wurde. Solche Ausnahmefälle sind auf das erforderliche Minimum zu beschränken und zeitnah zu löschen.

8. Unterauftragsverarbeiter

8.1 Der Kunde erteilt Thalassa eine allgemeine schriftliche Genehmigung zur Beauftragung der in Anlage 3 aufgeführten Unterauftragsverarbeiter.

8.2 Thalassa informiert den Kunden mindestens 30 Tage vor dem geplanten Einsatz eines neuen oder dem Austausch eines bestehenden Unterauftragsverarbeiters, soweit der neue Dienstleister personenbezogene Kundendaten verarbeitet. Die Information kann per E-Mail oder über einen dauerhaft erreichbaren Subprocessor-Update-Kanal erfolgen.

8.3 Der Kunde kann innerhalb dieser Frist aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Können die Parteien keine angemessene Lösung finden, kann der Kunde die konkret betroffene Funktion oder, wenn dies technisch nicht möglich ist, den Hauptvertrag nach den dort vorgesehenen Regeln beenden.

8.4 Thalassa verpflichtet jeden Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die den wesentlichen Anforderungen dieser AVV entsprechen, und bleibt gegenüber dem Kunden für dessen datenschutzrechtliche Leistung verantwortlich.

9. Verarbeitung in der EU / EWR und Drittlandübermittlungen

9.1 Die produktive Thalassa-Infrastruktur für Meeting-Inhaltsdaten ist grundsätzlich auf europäische AWS-Regionen auszurichten. Für Amazon Bedrock ist eine EU-geografische oder eine einzelne EU-Region zu verwenden; globale Inference-Profile dürfen für Kundendaten unter dieser AVV nicht als Standardkonfiguration eingesetzt werden. Eine Ausnahme hiervon besteht, soweit der Nutzer die Websuche anfordert und die hierfür erforderliche KI-Antwortgenerierung über die direkte API von Anthropic PBC erfolgt; Audiodaten und das laufende Transkript sind von dieser Ausnahme nicht erfasst.

9.2 Für Speech-to-Text ist der Deepgram-EU-Endpunkt zu verwenden, soweit er die erforderliche Funktion unterstützt. Ein automatischer Fallback auf einen nicht-europäischen Speech-to-Text-Endpunkt ist für Kundendaten unter dieser AVV nicht zulässig, sofern nicht zuvor eine geeignete Drittlandtransfergrundlage eingerichtet und der Kunde entsprechend informiert wurde.

9.3 Soweit ein Unterauftragsverarbeiter in einem Drittland ansässig ist oder aus einem Drittland rechtlich auf personenbezogene Daten zugreifen kann, stellt Thalassa vor Beginn der Verarbeitung eine Rechtsgrundlage nach Kapitel V DSGVO sicher. Soweit keine Angemessenheitsentscheidung greift, werden insbesondere die

Standardvertragsklauseln der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914 in der einschlägigen Modulkonstellation verwendet und erforderlichenfalls zusätzliche Maßnahmen umgesetzt.

9.4 Für Deepgram, Inc. als US-amerikanischem Unterauftragsverarbeiter ist ein DPA einschließlich geeigneter Standardvertragsklauseln abzuschließen. Zusätzlich ist die Nutzung von Kundendaten für Modellverbesserung, Benchmarking oder vergleichbare Sekundärzwecke vertraglich und technisch zu deaktivieren.

9.5 Für Anthropic PBC als US-amerikanischem Unterauftragsverarbeiter ist die Verarbeitung über die direkte API ausschließlich für die vom Nutzer angeforderte Websuche freigegeben. Hierfür gilt der Anthropic-Auftragsverarbeitungsvertrag einschließlich der darin einbezogenen Standardvertragsklauseln, der nach den für den Dienst geltenden Commercial Terms of Service Vertragsbestandteil ist. Die Nutzung der übermittelten Kundendaten für Modelltraining oder vergleichbare Modellverbesserungszwecke ist auszuschließen. Übermittelt werden nur die für diese Funktion erforderlichen Inhalte gemäß Anlage 1; Audiodaten und das laufende Transkript werden nicht an Anthropic PBC übermittelt.

9.6 Wird ein KI-Modell über Amazon Bedrock bereitgestellt, erfolgt die Auftragsverarbeitung gegenüber Thalassa über AWS. Soweit AWS nach seiner jeweiligen Produktkonfiguration Eingaben und Ausgaben nicht an den Modellanbieter weitergibt, wird der Modellanbieter nicht allein wegen der Bereitstellung des Modells als Empfänger von Kundendaten behandelt. Der direkte API-Aufruf von Anthropic PBC für die vom Nutzer angeforderte Websuche ist nach Maßgabe von Ziffer 9.5 und Anlage 3 freigegeben. Wird darüber hinaus die direkte API eines weiteren Modellanbieters eingesetzt, muss dieser vor Produktiveinsatz in Anlage 3 aufgenommen und ein geeigneter AVV-/Transfermechanismus eingerichtet werden.

10. Unterstützung bei Betroffenenrechten

10.1 Thalassa unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und soweit technisch möglich durch geeignete Maßnahmen bei der Erfüllung von Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.

10.2 Geht ein Betroffenenersuchen unmittelbar bei Thalassa ein und betrifft es Daten, die Thalassa ausschließlich im Auftrag eines Kunden verarbeitet, leitet Thalassa das Ersuchen grundsätzlich an den betreffenden Kunden weiter und beantwortet es nicht eigenständig, soweit keine gesetzliche Verpflichtung zur unmittelbaren Bearbeitung besteht.

11. Datenschutzverletzungen

11.1 Thalassa informiert den Kunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, die unter diese AVV fällt, unverzüglich und grundsätzlich innerhalb von 24 Stunden, soweit zu diesem Zeitpunkt ausreichende Informationen vorliegen.

11.2 Die Meldung enthält, soweit verfügbar, eine Beschreibung der Art des Vorfalls, betroffene Datenkategorien und Personengruppen, wahrscheinliche Folgen, bereits ergriffene oder geplante Gegenmaßnahmen sowie eine Kontaktstelle für Rückfragen.

11.3 Die Meldung stellt kein Anerkenntnis einer Pflichtverletzung dar. Thalassa dokumentiert relevante Sicherheitsvorfälle und unterstützt den Kunden bei gesetzlichen Melde- und Benachrichtigungspflichten.

12. Datenschutz-Folgenabschätzung und Behördenkonsultation

Soweit die Verarbeitung durch Thalassa für eine Datenschutz-Folgenabschätzung des Kunden relevant ist, stellt Thalassa dem Kunden die vernünftigerweise verfügbaren technischen und organisatorischen Informationen zur Verfügung und unterstützt ihn in angemessenem Umfang. Entsprechendes gilt für eine gegebenenfalls erforderliche vorherige Konsultation der zuständigen Aufsichtsbehörde.

13. Rückgabe und Löschung

13.1 Nach Beendigung der Verarbeitungsleistungen löscht oder gibt Thalassa personenbezogene Daten nach Wahl des Kunden zurück, soweit sie nicht bereits nach dem Produktdesign automatisch gelöscht wurden und keine gesetzliche Aufbewahrungspflicht entgegensteht.

13.2 Meeting-Audio, transiente Transkripte, Screenshots und generierte Meeting-Inhalte werden nicht als dauerhafte Meetingakte in der Thalassa-Cloud gespeichert. Technisch unvermeidbare flüchtige Verarbeitungs- oder Pufferkopien werden nach Abschluss des jeweiligen Verarbeitungsvorgangs automatisch entfernt; Inhaltsdaten sollen nicht Bestandteil dauerhafter Logs sein.

13.3 Vom Kunden lokal gespeicherte Wissensbasen, lokale Transkripte, Exporte oder lokal gespeicherte Debriefings liegen außerhalb der Cloud-Löschung durch Thalassa und werden vom Kunden auf seinen Endgeräten verwaltet.

14. Nachweise und Auditrechte

14.1 Thalassa stellt dem Kunden auf Anfrage die Informationen zur Verfügung, die vernünftigerweise erforderlich sind, um die Einhaltung dieser AVV nachzuweisen. Vorhandene unabhängige Prüfberichte, Zertifizierungen und Sicherheitsdokumentationen können vorrangig als Nachweis verwendet werden.

14.2 Der Kunde kann bei konkreten Anhaltspunkten für eine wesentliche Nichtkonformität oder wenn gesetzlich erforderlich ein Audit durchführen oder durch einen unabhängigen, zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Audits sind mit angemessener Vorankündigung, während üblicher Geschäftszeiten und so durchzuführen, dass Betrieb, Sicherheit und Vertraulichkeit anderer Kunden nicht beeinträchtigt werden.

14.3 Soweit ein Audit ausschließlich aufgrund eines vom Kunden gewünschten Sonderumfangs entsteht und keine wesentliche Pflichtverletzung von Thalassa festgestellt wird, können angemessene Zusatzkosten nach vorheriger Abstimmung dem Kunden berechnet werden.

15. Besondere Datenkategorien, Meetingteilnehmer und Minderjährige

15.1 Der Dienst ist nicht darauf ausgelegt, besondere Kategorien personenbezogener Daten gezielt zu erheben. Solche Daten können jedoch aufgrund des offenen Inhalts von Meetings, Screenshots oder Dokumentauszügen beiläufig verarbeitet werden. Der Kunde stellt sicher, dass hierfür eine zulässige Rechtsgrundlage bzw. Ausnahme nach Art. 9 DSGVO oder nach sonstigem anwendbarem Recht besteht.

15.2 Der Kunde ist dafür verantwortlich, Meetingteilnehmer und sonstige betroffene Personen in der jeweils erforderlichen Form über die Nutzung von Speech-to-Text- und KI-Funktionen zu informieren und, soweit erforderlich, wirksame Einwilligungen oder andere Rechtsgrundlagen einzuholen.

15.3 Thalassa erstellt keine Voiceprints, führt keine biometrische Sprecheridentifikation zur eindeutigen Identifizierung einer Person durch und verwendet die Meeting-Audiodaten ausschließlich für Speech-to-Text, soweit keine andere Funktion ausdrücklich vereinbart wird.

15.4 Thalassa bewertet im normalen Meetingbetrieb keine Persönlichkeit, Emotionen, Beschäftigtenleistung, Prüfungsleistung oder Eignung einer Person. Soweit ein separater Übungsmodus objektive Rückmeldungen zu Antworten bietet, darf dieser nicht als automatisierte Entscheidung mit rechtlicher oder vergleichbar erheblicher Wirkung ausgestaltet werden.

15.5 Bei Minderjährigen obliegt dem Kunden die Einhaltung der jeweils anwendbaren Alters-, Einwilligungs- und Informationspflichten. Diese AVV begründet keine Berechtigung zur eigenständigen B2C-Registrierung von Kindern.

16. Weitere anwendbare Datenschutzgesetze

16.1 Soweit auf die Verarbeitung neben der DSGVO weitere Datenschutzgesetze anwendbar sind, sind die Parteien verpflichtet, diese im Rahmen ihrer jeweiligen Rolle einzuhalten. Hierzu können insbesondere UK GDPR und Data Protection Act 2018, das Schweizer Datenschutzgesetz, US-amerikanische bundesstaatliche Datenschutzgesetze (einschließlich CCPA/CPRA, soweit anwendbar), kanadische, australische, japanische, koreanische und singapurische Datenschutzvorschriften gehören.

16.2 Soweit das Recht einer Rechtsordnung zusätzliche zwingende Processor-/Service-Provider-Pflichten vorsieht, gelten diese ergänzend. Für beschränkte Übermittlungen aus dem Vereinigten Königreich oder der Schweiz werden die jeweils erforderlichen Transferinstrumente bzw. Anpassungen verwendet.

16.3 Für Zwecke des CCPA/CPRA, soweit anwendbar, verarbeitet Thalassa personenbezogene Informationen nur für die vertraglich festgelegten Geschäftszwecke, verkauft oder teilt sie nicht für kontextübergreifende Werbung und kombiniert sie nicht mit personenbezogenen Informationen aus anderen Quellen, soweit dies nicht gesetzlich zulässig und zur Erbringung des Dienstes erforderlich ist.

16.4 Die regionalen Ergänzungen in den Anlagen 4A bis 4C gelten automatisch, soweit das jeweilige Datenschutzrecht auf den Kunden, die betroffenen Personen, die Verarbeitung oder eine internationale Datenübermittlung anwendbar ist. Soweit eine regionale Ergänzung zwingende strengere Anforderungen enthält, geht sie für den betreffenden Sachverhalt den allgemeinen Bestimmungen dieser AVV vor.

17. Haftung, Laufzeit und Beendigung

17.1 Die Haftung der Parteien richtet sich nach den zwingenden gesetzlichen Vorschriften und, soweit zulässig, nach den Haftungsregelungen des Hauptvertrags. Keine Bestimmung dieser AVV beschränkt Rechte betroffener Personen oder behördliche Befugnisse.

17.2 Diese AVV tritt mit Annahme in Kraft und gilt so lange, wie Thalassa im Auftrag des Kunden personenbezogene Daten verarbeitet.

17.3 Endet der Hauptvertrag, endet diese AVV nach Abschluss aller datenschutzrechtlich erforderlichen Lösch-, Rückgabe- und Nachweispflichten.

18. Rangfolge, anwendbares Recht und Änderungen

18.1 Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag hat diese AVV hinsichtlich Datenschutz und Auftragsverarbeitung Vorrang. Zwingende Standardvertragsklauseln oder sonstige zwingende Transferinstrumente gehen entgegenstehenden Bestimmungen dieser AVV vor.

18.2 Soweit der Hauptvertrag keine andere wirksame Rechtswahl enthält, gilt ungarisches Recht unter Vorrang des unmittelbar anwendbaren Unionsrechts. Zwingende Datenschutzvorschriften und Zuständigkeiten der Aufsichtsbehörden bleiben unberührt.

18.3 Änderungen dieser AVV bedürfen der Textform oder einer anderen elektronisch dokumentierten Form. Rein technische Aktualisierungen der Anlagen, insbesondere Sicherheitsmaßnahmen oder Subprocessor-Listen, dürfen nach dem in dieser AVV beschriebenen Änderungs- und Informationsverfahren vorgenommen werden, sofern das Schutzniveau nicht wesentlich abgesenkt wird.

19. Elektronischer Abschluss

19.1 Die Parteien vereinbaren, dass diese AVV elektronisch abgeschlossen werden kann. Die elektronische Annahme kann insbesondere durch eine elektronische Signatur oder durch ein eindeutig protokolliertes Click-to-Accept-Verfahren erfolgen.

19.2 Das elektronische Abschlussprotokoll soll mindestens die Identität bzw. das Kundenkonto, Firmenname, Name und Funktion der handelnden Person, die bestätigte Vertretungsberechtigung, E-Mail-Adresse, Datum

und Uhrzeit der Annahme, die angenommene Dokumentversion sowie einen manipulationsgeschützten Nachweis der angenommenen Fassung enthalten.

19.3 Nach Annahme erhält der Kunde eine dauerhafte Kopie der AVV oder einen dauerhaft verfügbaren Download-Link zur konkret angenommenen Version. Thalassa bewahrt den Nachweis des Vertragsschlusses entsprechend den gesetzlichen und vertraglichen Anforderungen auf.

Anlage 1 – Beschreibung der Verarbeitung

Merkmal	Beschreibung
Gegenstand	Bereitstellung von Thalassa Assistant als Echtzeit-Meeting-Assistent.
Zweck	Speech-to-Text, kontextbezogene KI-Antwortgenerierung, RAG aus lokaler Wissensbasis, Screenshotanalyse, Briefing/Debriefing, Abruf von Kalender-, Kontakt-, E-Mail- und Dokumentdaten aus vom Nutzer verbundenen Systemen für Briefing und Antworten, sowie – soweit vom Nutzer angefordert – KI-Antwortgenerierung mit Websuche über Anthropic PBC und technisch erforderliche Dienstbereitstellung.
Dauer	Laufzeit des Hauptvertrags; Meeting-Inhaltsdaten grundsätzlich nur transient während der jeweiligen Verarbeitung.
Betroffene Personen	Nutzer des Kunden; Beschäftigte; Bewerber; Meetingteilnehmer; Kunden, Interessenten, Berater, Rechts-/Finanzkontakte und andere Personen, deren Daten in Meetinginhalten, Screenshots, Dokumentauszügen oder in Kalendereinträgen, Kontakten, E-Mails und Dokumenten verbundener Systeme erscheinen.
Datenarten	Audio-/Sprachdaten; Gesprächsinhalte; transiente Transkripte; Namen/Kontaktdaten, soweit im Inhalt enthalten; Screenshots; ausgewählte Dokumentauszüge; Kalendereinträge, Kontaktdaten, E-Mail-Inhalte und Dokumentauszüge aus verbundenen Systemen; verschlüsselte Zugangsschlüssel (OAuth-Tokens) zu diesen Systemen; technische Sitzungs- und Request-Metadaten; generierte Antworten; ggf. besondere Datenkategorien, wenn sie vom Kunden oder Meetingteilnehmer eingebracht werden.
Verarbeitungsvorgänge	Erfassen/Streamen, Übermitteln, Speech-to-Text, Pseudonymisieren/Minimieren, temporäres Puffern, Retrieval, Abrufen aus verbundenen Systemen, Anlegen von E-Mail-Entwürfen auf Weisung des Nutzers, KI-Inferenz, nutzerangeforderte Websuche, Anzeigen, Generieren, technisch erforderliches Zwischenspeichern und Löschen.
Voice-Biometrie	Keine Voiceprints und keine biometrische Sprecheridentifikation zur eindeutigen Identifizierung.
Profiling / Bewertung	Keine reguläre Bewertung von Persönlichkeit, Emotion, Mitarbeiterleistung, Prüfungsleistung oder Eignung; kein automatisiertes Entscheiden mit rechtlicher oder vergleichbar erheblicher Wirkung als Standardfunktion.

A. Datenfluss und Speicherlogik

Mikrofon/Systemaudio wird lokal erfasst und für Speech-to-Text an Deepgram übertragen. Für produktive EU-Nutzung ist der Deepgram-EU-Endpunkt zu verwenden.

Das erzeugte Transkript wird nur transient für die laufende Sitzung bzw. Anfrage verarbeitet. Es wird nicht als vollständige Meetingakte dauerhaft in der Thalassa-Cloud gespeichert.

Kundendokumente/PDFs und die lokale Wissensbasis verbleiben grundsätzlich auf dem Endgerät. Für die KI-Antwort können jedoch ausgewählte, durch lokales Retrieval bestimmte Textauszüge und Kontextpassagen an die KI-Verarbeitung übermittelt werden. Daher darf nicht behauptet werden, dass sämtliche Dokumentinhalte ausnahmslos das Endgerät nie verlassen.

Screenshots werden nur bei aktivierter/manuell ausgelöster Funktion und nur für die jeweilige Anfrage übertragen und verarbeitet.

Soweit der Nutzer die Websuche anfordert, wird die für die KI-Antwort bestimmte Anfrage über die direkte API von Anthropic PBC verarbeitet. Dabei werden die Nutzerfrage, die Vorbereitungsangaben des Nutzers und die aus der lokalen Wissensbasis durch Retrieval ausgewählten Dokumentauszüge übermittelt. Audiodaten und das laufende Transkript werden hierbei nicht an Anthropic PBC übermittelt; die Speech-to-Text-Verarbeitung bleibt beim Deepgram-EU-Endpunkt.

Generierte Antworten und Debriefings werden nicht zentral als vollständige Meetinghistorie gespeichert, sofern keine ausdrücklich vereinbarte Funktion dies vorsieht. Der Nutzer kann Ergebnisse lokal speichern oder exportieren.

Verbindungen zu Microsoft 365, Google und Anbietern mit MCP-Schnittstelle richtet der Nutzer freiwillig selbst ein und kann sie jederzeit trennen; bei Geschäftskonten kann die Zustimmung einer Administration des Kunden vorgeschaltet sein. Abgerufen wird nur, was eine konkrete Vorbereitung oder ein laufendes Gespräch braucht. Kalender-, Kontakt- und E-Mail-Inhalte laufen transient über das Backend in Frankfurt und werden dort nicht gespeichert; Dateiinhalte aus OneDrive, SharePoint und Google Drive verarbeitet die App auf dem Endgerät und verwirft sie nach dem Gespräch, bei einem Kontowechsel und beim Trennen. Für die KI-Antwort gilt derselbe Weg wie für Dokumentauszüge aus der lokalen Wissensbasis. Die Inhalte werden nicht zum Training verwendet und nicht in die Wissensbasis übernommen. Thalassa versendet keine E-Mails; auf Weisung des Nutzers legt sie lediglich einen Entwurf im Postfach des Nutzers an. Auf Gmail greift Thalassa nicht zu.

Die von Microsoft oder Google nach Zustimmung ausgestellten Zugangsschlüssel speichert Thalassa mit AES-256-GCM verschlüsselt im Backend in Frankfurt, gebunden an Konto und Anbieter. Beim Trennen der Verbindung werden sie gelöscht und ein Google-Schlüssel zusätzlich bei Google widerrufen; bei Löschung des Kontos werden sie mit allen übrigen Kontodaten gelöscht. Daten aus Google-Schnittstellen unterliegen der Google API Services User Data Policy einschließlich der Limited-Use-Anforderungen.

Anbieter mit MCP-Schnittstelle verbindet die Desktop-App unmittelbar mit dem vom Kunden konfigurierten Server; Zugangsdaten hierfür verbleiben beim Kunden. Abgerufener Text wird auf dem Endgerät indexiert und durchsucht; ausgewählte Auszüge folgen für Antworten und Briefings dem bestehenden Anfrageweg. Jeder Werkzeugaufruf erfolgt erst nach Bestätigung durch den Nutzer.

Account-, Abrechnungs- und allgemeine Nutzungsmetadaten können getrennt als Daten in eigener Verantwortlichkeit von Thalassa gespeichert werden; sie fallen nicht automatisch unter diese Anlage.

B. Aufbewahrung

Datenkategorie	Cloud-Aufbewahrung	Regel
Roh-Audio	Keine dauerhafte Speicherung durch Thalassa	Streaming-Verarbeitung; Deepgram-Vertrag/Konfiguration muss Sekundärnutzung und nicht erforderliche Speicherung ausschließen.
Transkript	Keine dauerhafte Speicherung	Transient während Session/Request; automatische Löschung nach Ende der Verarbeitung.
Screenshots	Keine dauerhafte Speicherung	Transient pro Anfrage; automatische Löschung nach Verarbeitung.
RAG-Dokumentauszüge	Keine dauerhafte Inhaltsablage als Dokumentenarchiv	Nur für Inferenz; keine Trainingsnutzung.
Generierte Antworten	Keine dauerhafte Meetingakte	Nur transient, sofern Nutzer nicht lokal speichert/exportiert.
Technische Logs	Metadaten nur soweit erforderlich	Keine Meeting-Inhalte in Standardlogs; Aufbewahrungsfristen nach Sicherheits-/Betriebskonzept.
Kalender, Kontakte, E-Mails	Keine dauerhafte Speicherung	Transient je Vorbereitung/Anfrage über das

Datenkategorie	Cloud-Aufbewahrung	Regel
verbundener Systeme		Backend; automatische Löschung nach Verarbeitung.
Dateiinhalte verbundener Systeme	Keine Speicherung in der Cloud	Verarbeitung auf dem Endgerät; verworfen nach dem Gespräch, bei Kontowechsel und beim Trennen.
Zugangsschlüssel (OAuth-Tokens)	Verschlüsselt (AES-256-GCM), Frankfurt	Bis zum Trennen der Verbindung (Löschung, bei Google zusätzlich Widerruf) oder bis zur Kontolöschung.
Quellenangaben einer Vorbereitung	Nur Metadaten (Dateiname, Link, Fassung, Abrufzeit)	Keine Inhalte; Lebensdauer wie das zugehörige Briefing des Nutzers.

Anlage 2 – Technische und organisatorische Maßnahmen (TOM)

1. Zugriffskontrolle

Rollen- und berechtigungsbasierte Zugriffe nach Least-Privilege-Prinzip.

MFA für privilegierte Administrationszugänge.

Regelmäßige Überprüfung und Entzug nicht mehr benötigter Zugriffsrechte.

Keine Weitergabe produktiver Zugangsdaten; Secrets in geeigneten Secret-Management-Systemen.

2. Übertragungssicherheit

Verschlüsselung von Daten während der Übertragung mit aktuellen TLS-Verfahren (mindestens TLS 1.2, soweit technisch unterstützt).

Bevorzugte Nutzung privater AWS-Netzwerkpfade/PrivateLink für interne Cloud-Kommunikation, soweit technisch sinnvoll.

Keine unverschlüsselte Übertragung von Meeting-Inhaltsdaten über öffentliche Netze.

3. Verschlüsselung gespeicherter Daten

Cloud-Metadaten und sonstige persistente personenbezogene Daten werden verschlüsselt gespeichert, soweit der jeweilige AWS-Dienst dies unterstützt.

Schlüsselverwaltung über AWS KMS oder gleichwertige Verfahren; Zugriff auf Schlüssel nach Least-Privilege.

Meeting-Inhaltsdaten sollen nicht persistent gespeichert werden; damit wird die Angriffsfläche zusätzlich reduziert.

Zugangsschlüssel zu verbundenen Systemen (OAuth-Tokens) werden vor der Ablage in der Datenbank mit AES-256-GCM verschlüsselt; der Chiffretext ist an Konto und Anbieter gebunden, sodass ein aus der Datenbank kopierter Wert gegen ein anderes Konto nicht verwendbar ist. Zugriffsrechte werden nach dem Grundsatz der geringsten Berechtigung angefordert; ein Recht zum Versand von E-Mails wird nicht angefordert.

4. Datenminimierung und Pseudonymisierung

Übermittlung an KI-Dienste nur des für die konkrete Antwort erforderlichen Kontextes.

Entfernung oder Ersetzung direkt identifizierender Angaben, soweit dies ohne Funktionsverlust möglich ist.

Pseudonymisierte Daten werden weiterhin als personenbezogene Daten behandelt.

Keine Trainingsnutzung von Kundendaten.

5. Logging und Monitoring

Sicherheits- und Betriebslogs erfassen nach Möglichkeit keine Meetinginhalte.

Monitoring auf Verfügbarkeit, unautorisierte Zugriffe und sicherheitsrelevante Anomalien.

Administrative Änderungen und sicherheitsrelevante Ereignisse werden nachvollziehbar protokolliert.

6. Mandantentrennung

Logische Trennung von Kunden-/Nutzerdaten durch eindeutige Tenant-/User-Zuordnung und Zugriffskontrollen.

Keine absichtliche Vermischung von Meetinginhalten verschiedener Kunden.

Tests der Autorisierungs- und Tenant-Grenzen vor Produktivfreigaben.

7. Sichere Entwicklung

Code-Review und kontrollierte Freigabeprozesse für produktionsrelevante Änderungen.

Abhängigkeits- und Schwachstellenmanagement mit zeitnaher Behebung kritischer Sicherheitslücken.

Trennung von Entwicklungs-, Test- und Produktivumgebungen, soweit personenbezogene Produktivdaten betroffen sind.

Keine Nutzung realer Kundendaten in Entwicklung/Test, sofern nicht zwingend erforderlich und gesondert abgesichert.

8. Verfügbarkeit und Wiederherstellung

Geeignete Backup- und Wiederherstellungsverfahren für persistente Betriebs- und Accountdaten.

Wiederanlauf- und Incident-Response-Verfahren für wesentliche Systeme.

Meeting-Inhaltsdaten werden wegen der transienten Verarbeitung grundsätzlich nicht als Backupbestand vorgesehen.

9. Incident Response

Dokumentierter Prozess zur Erkennung, Bewertung, Eindämmung und Behebung von Sicherheitsvorfällen.

Interne Eskalationswege und Verantwortlichkeiten.

Prozess zur Kundenbenachrichtigung nach Abschnitt 11 dieser AVV.

10. Lieferantenkontrolle

DPA/AVV mit Unterauftragsverarbeitern vor produktiver Verarbeitung personenbezogener Kundendaten.

Prüfung der Transfermechanismen für Drittlandanbieter.

Deepgram: EU-Endpunkt verwenden; DPA/SCC abschließen; Modellverbesserungs-/Benchmarking-Nutzung deaktivieren.

Amazon Bedrock: EU-Region bzw. EU-Geo-Inference verwenden; keine globale Inference als Standard für Kundendaten.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Anbieter / Sitz / Rolle	Zweck	Transfermechanismus / Besonderheit
Amazon Web Services (AWS) AWS-Gruppe / einschlägige Vertragsgesellschaft Cloud-Unterauftragsverarbeiter	Hosting, Authentifizierung, Backend-/Datenbankdienste und Amazon Bedrock KI-Inferenz	AWS-DPA; einschlägige Transfermechanismen für Drittlandzugriffe. Bedrock-Eingaben/-Ausgaben dürfen nicht an Modellanbieter weitergegeben werden.

Anbieter / Sitz / Rolle	Zweck	Transfermechanismus / Besonderheit
Deepgram, Inc. (USA) Unterauftragsverarbeiter	Echtzeit-Speech-to-Text	Deepgram-DPA + SCC (Modul 3, soweit einschlägig); keine Modellverbesserung; kein Benchmarking; kein Nicht-EU-Fallback ohne vorherige Compliance-Prüfung.
Anthropic PBC (USA) Unterauftragsverarbeiter	KI-Antwortgenerierung mit Websuche, soweit vom Nutzer angefordert	Anthropic-DPA einschließlich Standardvertragsklauseln, als Bestandteil der Commercial Terms of Service; keine Nutzung der Eingaben für Modelltraining.
DeepL SE (Köln, Deutschland) Unterauftragsverarbeiter	Live-Übersetzung, soweit vom Nutzer angefordert	DeepL-Auftragsverarbeitungsvertrag (DeepL API Pro); keine Nutzung der Eingaben für Modelltraining; Drittlandübermittlungen nur nach Kapitel V DSGVO (DeepL-DPA einschließlich Standardvertragsklauseln).

Hinweis: Ein direkter Aufruf eines Modellanbieters ist nur für die in dieser Anlage ausdrücklich aufgeführten Anbieter und Zwecke freigegeben. Anthropic PBC ist für die vom Nutzer angeforderte Websuche nach den vorstehenden Bedingungen aufgenommen. Jeder weitere direkte API-Anbieter muss vor Produktiveinsatz in diese Anlage aufgenommen und die erforderliche DPA-/Drittlandtransferprüfung abgeschlossen werden.

Microsoft, Google und Anbieter mit MCP-Schnittstelle sind keine Unterauftragsverarbeiter von Thalassa. Sie sind die vom Kunden selbst beauftragten Anbieter; Thalassa greift auf die dort liegenden Daten nur mit Zustimmung des Nutzers und im Rahmen der vom Kunden erteilten Berechtigungen lesend bzw. – bei E-Mail-Entwürfen – im Postfach des Nutzers zu. Das Vertragsverhältnis zu diesen Anbietern und die Rechtsgrundlage für die dortige Verarbeitung bleiben Sache des Kunden.

Anlage 4 – Internationale Datenübermittlungen und regionale Ergänzungen

A. EWR: Für Übermittlungen aus dem EWR in ein Drittland gelten die Anforderungen der Art. 44 ff. DSGVO. Soweit erforderlich, werden die Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 in der jeweils passenden Modulkonstellation einbezogen.

B. Vereinigtes Königreich: Soweit UK GDPR gilt und eine „restricted transfer“ vorliegt, verwenden die Parteien den jeweils gültigen UK International Data Transfer Addendum oder ein anderes zulässiges Transferinstrument.

C. Schweiz: Soweit das Schweizer Datenschutzgesetz anwendbar ist, werden die EU-Standardvertragsklauseln erforderlichenfalls so ergänzt, dass schweizerische Begriffe, Aufsichtsbehörden und anwendbare Regelungen abgedeckt sind.

D. USA / Kalifornien: Soweit CCPA/CPRA anwendbar ist, handelt Thalassa hinsichtlich der im Auftrag verarbeiteten Kundendaten als Service Provider/Contractor im gesetzlich vorgesehenen Umfang und nutzt die Daten nicht außerhalb der vertraglich festgelegten Geschäftszwecke.

E. Weitere Staaten: Für Kanada, Australien, Japan, Republik Korea, Singapur und andere Zielmärkte gelten zusätzlich die zwingenden lokalen Datenschutzvorschriften. Diese Anlage soll einen globalen Mindeststandard schaffen, ersetzt jedoch keine zwingend vorgeschriebene lokale Zusatzvereinbarung, falls eine Rechtsordnung eine solche verlangt.

F. Anthropic PBC / nutzerangeforderte Websuche: Soweit der Nutzer die Websuche anfordert, können die Nutzerfrage, die Vorbereitungsangaben des Nutzers und die aus der lokalen Wissensbasis abgerufenen Dokumentauszüge an Anthropic PBC in den Vereinigten Staaten übermittelt werden. Audiodaten und das laufende Transkript sind hiervon nicht erfasst. Die Übermittlung erfolgt auf Grundlage des Anthropic-DPA einschließlich der darin einbezogenen Standardvertragsklauseln und unter Ausschluss einer Nutzung der übermittelten Kundendaten für Modelltraining oder vergleichbare Modellverbesserungszwecke.

Anlage 4A – Schweiz (Swiss FADP Addendum)

Diese Anlage gilt automatisch, soweit das Schweizer Bundesgesetz über den Datenschutz (DSG/FADP) auf den Kunden, eine betroffene Person, die Verarbeitung oder eine Datenbekanntgabe ins Ausland anwendbar ist.

CH-1. Begriffe und Rangfolge. Begriffe wie Personendaten, Bearbeiten, Verantwortlicher, Auftragsbearbeiter und besonders schützenswerte Personendaten sind im Anwendungsbereich dieser Anlage nach dem Schweizer DSG auszulegen. Die allgemeinen Schutzpflichten dieser AVV gelten zusätzlich. Soweit DSG und DSGVO parallel anwendbar sind, werden beide Regelwerke eingehalten; zwingende gesetzliche Anforderungen bleiben unberührt.

CH-2. Auftragsbearbeitung. Thalassa bearbeitet Personendaten, die unter diese AVV fallen, nur für die dokumentierten Zwecke und Weisungen des Kunden, gewährleistet angemessene Datensicherheit, Vertraulichkeit, Subprocessor-Kontrolle und unterstützt den Kunden bei der Wahrnehmung der Rechte betroffener Personen nach dem Schweizer DSG.

CH-3. Datenbekanntgabe ins Ausland. Eine Bekanntgabe aus der Schweiz in einen Staat mit angemessenem Datenschutzniveau kann auf die jeweilige Angemessenheitsregelung nach Schweizer Recht gestützt werden. Für Bekanntgaben in Staaten ohne angemessenes Schutzniveau werden geeignete Garantien nach Art. 16 DSG eingesetzt, insbesondere vom EDÖB anerkannte Standarddatenschutzklauseln oder ein anderer zulässiger Transfermechanismus.

CH-4. Schweizer Anpassungen der EU-SCC. Soweit die Standardvertragsklauseln der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914 für eine dem Schweizer DSG unterliegende Übermittlung verwendet werden, wählen die Parteien grundsätzlich den DSGVO-Schutzstandard für die gesamte erfasste Übermittlung. Der EDÖB bleibt für die Einhaltung des Schweizer DSG zuständig; bei paralleler DSGVO-Anwendbarkeit besteht die gesetzliche Zuständigkeit der einschlägigen EU-Aufsichtsbehörde daneben fort.

CH-5. Gerichtsschutz schweizerischer betroffener Personen. Verweise der EU-SCC auf einen „Mitgliedstaat“ dürfen nicht so ausgelegt werden, dass eine betroffene Person mit gewöhnlichem Aufenthalt in der Schweiz daran gehindert wird, die ihr nach den SCC oder dem Schweizer DSG zustehenden Rechte vor einem nach Schweizer Recht zuständigen Gericht an ihrem gewöhnlichen Aufenthaltsort geltend zu machen.

CH-6. Anwendbares Recht der SCC. Soweit die EU-SCC zugleich zur Erfüllung von DSGVO-Anforderungen eingesetzt werden, bleibt für die SCC das dort wirksam gewählte Recht eines EU-Mitgliedstaats maßgeblich. Zwingende Rechte und Zuständigkeiten nach Schweizer DSG werden dadurch nicht ausgeschlossen.

CH-7. Schweiz-USA. Für Übermittlungen in die Vereinigten Staaten kann eine nach Schweizer Recht bestehende Angemessenheitsregelung für nach dem Swiss-U.S. Data Privacy Framework wirksam zertifizierte Empfänger genutzt werden, soweit deren Zertifizierung die konkrete Datenart und Verarbeitung abdeckt. Andernfalls sind geeignete Garantien, insbesondere die anerkannten SCC mit den erforderlichen Schweizer Ergänzungen, einzusetzen.

CH-8. Aufsichtsbehörde. Zuständige Schweizer Aufsichtsbehörde ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), soweit die betreffende Verarbeitung oder Übermittlung dem Schweizer DSG unterliegt.

Anlage 4B – Vereinigtes Königreich (UK GDPR Addendum)

Diese Anlage gilt automatisch, soweit UK GDPR, der Data Protection Act 2018 oder die britischen Regeln zu internationalen Datentransfers auf die Verarbeitung anwendbar sind.

UK-1. Begriffe. Verweise in dieser AVV auf DSGVO, personenbezogene Daten, Verantwortlichen, Auftragsverarbeiter, Aufsichtsbehörde und Betroffenenrechte umfassen im Anwendungsbereich dieser Anlage die entsprechenden Begriffe des UK GDPR und des Data Protection Act 2018.

UK-2. Übermittlung UK → Thalassa. Solange Ungarn bzw. der EWR durch britische Angemessenheitsregelungen vollständig erfasst ist, kann eine Übermittlung personenbezogener Daten von

einem britischen Kunden an Thalassa in Ungarn auf diese Angemessenheitsregelung gestützt werden; ein IDTA oder UK Addendum ist hierfür grundsätzlich nicht zusätzlich erforderlich.

UK-3. Restricted Transfers ohne Angemessenheit. Soweit eine nach UK GDPR beschränkte internationale Übermittlung nicht von einer britischen Angemessenheitsregelung erfasst ist, stellt die für die Übermittlung verantwortliche Partei vor Beginn der Übermittlung einen zulässigen Transfermechanismus sicher. Hierzu kann insbesondere das jeweils gültige, vom ICO genehmigte International Data Transfer Addendum zu den EU-SCC oder das International Data Transfer Agreement (IDTA) verwendet werden.

UK-4. EU-SCC + UK Addendum. Sind für denselben Datenfluss bereits die EU-SCC vereinbart, soll grundsätzlich das jeweils gültige ICO-Addendum zu diesen EU-SCC verwendet werden. Die zwingenden Bestandteile des offiziellen ICO-Addendums werden durch diese AVV nicht geändert oder ersetzt. Die Parteien vervollständigen die dort erforderlichen Angaben anhand dieser AVV, ihrer Anlagen und der konkreten Transferkonstellation.

UK-5. Transfer Risk Assessment / Data Protection Test. Soweit britisches Recht bei Verwendung geeigneter Garantien eine Transfer-Risikoprüfung bzw. den gesetzlichen Data-Protection-Test verlangt, führt die dafür verantwortliche Partei diese Prüfung durch. Thalassa stellt die vernünftigerweise verfügbaren Informationen über Empfänger, Verarbeitungsort, Sicherheitsmaßnahmen und Unterauftragsverarbeiter zur Verfügung.

UK-6. Vereinigte Staaten. Für eine beschränkte Übermittlung aus dem Vereinigten Königreich an einen US-Empfänger kann, soweit die gesetzlichen Voraussetzungen erfüllt sind, die UK Extension zum EU-U.S. Data Privacy Framework genutzt werden. Dies setzt insbesondere eine wirksame Zertifizierung des Empfängers für die UK Extension und die betroffene Datenkategorie voraus. Andernfalls sind geeignete Garantien einzusetzen.

UK-7. Aufsichtsbehörde. Zuständige britische Datenschutzaufsichtsbehörde ist das Information Commissioner's Office (ICO), soweit UK Datenschutzrecht auf die betreffende Verarbeitung Anwendung findet.

UK-8. Fortentwicklung. Wird ein vom ICO genehmigtes IDTA oder Addendum durch eine neue verbindliche Fassung ersetzt oder nach dem vorgesehenen Aktualisierungsmechanismus geändert, verwenden die Parteien für neue oder fortgesetzte Transfermechanismen die jeweils rechtlich wirksame Fassung innerhalb der einschlägigen Übergangsfristen.

Anlage 4C – Vereinigte Staaten (U.S. State Privacy Addendum)

Diese Anlage gilt automatisch, soweit ein anwendbares umfassendes Datenschutzgesetz eines US-Bundesstaats die Beziehung zwischen dem Kunden und Thalassa als Business/Controller und Service Provider/Contractor/Processor regelt. Für Kalifornien gelten insbesondere die nachstehenden CCPA/CPRA-Regelungen.

US-1. Rollen und Begriffe. Soweit das anwendbare US-Datenschutzrecht Begriffe wie Business, Controller, Service Provider, Contractor, Processor, Consumer, Personal Information, Personal Data, Sensitive Data, Sale, Sharing oder Targeted Advertising definiert, gelten diese Begriffe mit der Bedeutung des jeweils anwendbaren Gesetzes. Der Kunde handelt als Business/Controller und Thalassa als Service Provider/Contractor/Processor, soweit die gesetzlichen Voraussetzungen hierfür erfüllt sind.

US-2. Bestimmte Geschäftszwecke. Thalassa verarbeitet im Auftrag erhaltene personenbezogene Daten ausschließlich für die konkret vereinbarten Geschäftszwecke: Echtzeit-Speech-to-Text, kontextbezogene KI-Antwortgenerierung, RAG aus der lokalen Wissensbasis, Screenshotanalyse, Briefing/Debriefing, technische Bereitstellung der Sitzung sowie Sicherheit, Fehlerbehebung und Support, soweit diese Tätigkeiten zur Bereitstellung des Dienstes erforderlich oder vom Kunden angewiesen sind.

US-3. Kein Verkauf oder Teilen. Thalassa verkauft personenbezogene Kundendaten nicht und „teilt" sie nicht für Cross-Context Behavioral Advertising oder einen vergleichbaren gesetzlich definierten Werbezweck. Thalassa erhält keine Gegenleistung für die Offenlegung solcher Kundendaten zu eigenen Werbe- oder Datenhandelszwecken.

US-4. Zweckbindung. Thalassa darf personenbezogene Kundendaten nicht für Zwecke außerhalb der in US-2 beschriebenen Zwecke oder außerhalb der direkten Geschäftsbeziehung mit dem Kunden behalten, verwenden oder offenlegen, soweit das anwendbare Recht dies nicht ausdrücklich erlaubt.

US-5. Keine unzulässige Kombination. Thalassa kombiniert im Auftrag erhaltene personenbezogene Daten nicht mit personenbezogenen Daten aus anderen Kunden, aus eigenen Endnutzerbeziehungen oder aus Drittquellen, soweit eine solche Kombination nach dem anwendbaren US-Datenschutzrecht für Service Provider/Contractors/Processors unzulässig ist. Technisch notwendige Sicherheits-, Missbrauchs- und Integritätsprüfungen bleiben nur im gesetzlich zulässigen Umfang möglich.

US-6. Kein KI-Training und keine eigene Profilbildung. Personenbezogene Kundendaten werden nicht zum Training generativer Modelle, für fremde Modellverbesserung, personenbezogene Werbung, eigene Eignungsbewertungen oder eigene Profilbildung verwendet. Eine automatisierte Entscheidung mit rechtlicher oder ähnlich erheblicher Wirkung über eine betroffene Person ist keine Standardfunktion der Auftragsverarbeitung.

US-7. Consumer Rights. Thalassa unterstützt den Kunden in angemessenem Umfang bei anwendbaren Verbraucherrechten, insbesondere Auskunft/Zugang, Löschung, Berichtigung und Datenübertragbarkeit sowie bei gesetzlich einschlägigen Opt-out- oder Beschränkungsrechten. Thalassa antwortet auf Anträge betroffener Personen zu Auftragsdaten grundsätzlich nur nach Weisung des Kunden, sofern keine gesetzliche Pflicht zur direkten Antwort besteht.

US-8. Sensitive Data. Sensible personenbezogene Daten werden nur verarbeitet, soweit sie für die vom Kunden veranlasste Funktion erforderlich sind. Thalassa nutzt sensible Daten nicht, um außerhalb der beauftragten Dienstleistung Merkmale einer Person abzuleiten, und verwendet Sprachdaten nicht zur biometrischen Identifizierung oder Emotionserkennung.

US-9. Unterauftragsverarbeiter. Thalassa verpflichtet Unterauftragsverarbeiter, die personenbezogene Kundendaten verarbeiten, zu vertraglichen Beschränkungen, die mit den nach dieser Anlage für Thalassa geltenden Pflichten vereinbar sind. Thalassa bleibt für die Auswahl und vertragliche Einbindung der Unterauftragsverarbeiter nach Maßgabe dieser AVV verantwortlich.

US-10. Kontrolle und Nachweis. Der Kunde darf angemessene und verhältnismäßige Schritte unternehmen, um zu überprüfen, dass Thalassa die personenbezogenen Kundendaten im Einklang mit dieser Anlage und dem anwendbaren US-Datenschutzrecht verarbeitet. Hierfür gelten vorrangig die Nachweis- und Auditregelungen in Abschnitt 14 dieser AVV; weitergehende zwingende gesetzliche Kontrollrechte bleiben unberührt.

US-11. Mitteilung bei Nichtbefolgung. Stellt Thalassa fest, dass es eine auf diese Anlage anwendbare gesetzliche Pflicht als Service Provider, Contractor oder Processor nicht mehr erfüllen kann, informiert Thalassa den Kunden ohne unangemessene Verzögerung. Der Kunde kann angemessene Schritte verlangen, um eine unzulässige Nutzung zu stoppen und zu beheben.

US-12. California CCPA/CPRA. Soweit der CCPA/CPRA anwendbar ist, bestätigen die Parteien, dass die in US-2 beschriebenen Geschäftszwecke die begrenzten und bestimmten Zwecke der Offenlegung darstellen. Thalassa verpflichtet sich, die für Service Provider und Contractors geltenden gesetzlichen Beschränkungen einzuhalten, einschließlich des Verbots des Verkaufs oder Teilens, der Zweck- und Beziehungsbeschränkung, der gesetzlich erforderlichen Unterstützung des Kunden und der Pflicht, dem Kunden angemessene Überprüfungs- und Abhilfemaßnahmen zu ermöglichen.

US-13. Bestätigung. Thalassa bestätigt, die in dieser Anlage für Service Provider/Contractors/Processors festgelegten Beschränkungen verstanden zu haben und sie einzuhalten, soweit das jeweilige US-Datenschutzgesetz auf die Verarbeitung anwendbar ist.

US-14. Gesundheitsdaten / HIPAA. Diese AVV ist kein Business Associate Agreement nach HIPAA. Sofern nicht ausdrücklich eine gesonderte schriftliche Vereinbarung abgeschlossen wurde, darf der Kunde den Dienst nicht als HIPAA-regulierte Business-Associate-Lösung für geschützte Gesundheitsinformationen konfigurieren oder vermarkten.

US-15. Kinder- und B2C-Daten. Diese B2B-AVV ersetzt keine verbraucherbezogenen Informations-, Alters- oder Einwilligungspflichten nach COPPA oder sonstigem US-Kinder- und Verbraucherdatenschutzrecht.

Soweit der Kunde Daten Minderjähriger in die Auftragsverarbeitung einbringt, bleibt er für die hierfür erforderliche gesetzliche Befugnis und Information verantwortlich; Thalassa verarbeitet solche Daten ausschließlich im Rahmen der vereinbarten Dienstleistung.

Rechtsstand der regionalen Ergänzungen: 08.09.2026. Maßgeblich bleiben zwingende gesetzliche Änderungen und die jeweils gültigen offiziellen Transferinstrumente.

Anlage 5 – Elektronische Annahme / Signaturprotokoll

Kunde / Firma	[automatisch aus Account]
Name der handelnden Person	[Eingabe]
Funktion / Titel	[Eingabe]
E-Mail	[Eingabe / verifiziert]
Vertretungsberechtigung bestätigt	☐ Ja
AVV-Version	1.4 – 09.10.2026
Zeitpunkt der Annahme	[automatischer Zeitstempel]
Dokument-Hash / Audit-ID	[automatisch erzeugt]
Elektronische Annahme	☐ Ich akzeptiere diese AVV im Namen des oben genannten Kunden.

Empfohlener technischer Nachweis: unveränderbare Speicherung der angenommenen Dokumentversion oder ihres Hashes, Audit-ID, Zeitstempel, Account-/Kunden-ID, verifizierte E-Mail sowie Versand einer Kopie an den Kunden. IP-Adresse und Geräteinformationen sollten nur gespeichert werden, wenn dies für Beweis-/Sicherheitszwecke erforderlich und in der Datenschutzerklärung transparent beschrieben ist.

Annahme

Mit der elektronischen Annahme oder Unterzeichnung bestätigt die handelnde Person, zur Vertretung des Kunden berechtigt zu sein und diese AVV einschließlich ihrer Anlagen im Namen des Kunden abzuschließen.

Anlage 6 – OECD-Länderergänzungen zum Master-AVV

Diese Anlage ergänzt den Master-AVV für Kunden mit Sitz oder relevanter Datenverarbeitung in einem OECD-Mitgliedstaat. Sie ist als Länderanlage konzipiert und ändert den Haupttext des Master-AVV nicht, soweit nicht zwingendes nationales Datenschutzrecht eine abweichende Regel verlangt.

Stand der Länderabdeckung: 08.09.2026. Erfasst sind die 38 OECD-Mitgliedstaaten. Beitrittskandidaten und Partnerstaaten sind nicht erfasst, solange sie nicht OECD-Mitglied sind.

Aktivierungsregel: Der Abschnitt zu einem Land gilt automatisch, wenn der Kunde dort niedergelassen ist, betroffene Personen dort ansässig sind oder das jeweilige nationale Datenschutzrecht aus anderen Gründen zwingend auf die Verarbeitung Anwendung findet.

Rangfolge: Bei Widersprüchen gilt zwingendes lokales Datenschutzrecht vor dieser Anlage. Im Übrigen gelten der Master-AVV, die TOM, die Subprocessor-Regeln und die Drittlandtransferregeln unverändert fort. Für Schweiz, Vereinigtes Königreich und USA bleiben die bereits vorhandenen Detailanhänge vorrangig; die nachfolgenden Länderabschnitte dienen dort zusätzlich als Zuordnung und Kurzergänzung.

Keine lokale Rechtsberatung: Diese Länderanlage ist eine vertragliche Standarderweiterung. Sie ersetzt keine lokale Rechtsprüfung bei Enterprise-Kunden, regulierten Branchen, Gesundheitsdaten, Beschäftigtendaten, Kindern, Bildungs-/Prüfungssituationen oder behördlichen Kunden.

Länderindex: Australien; Österreich; Belgien; Kanada; Chile; Kolumbien; Costa Rica; Tschechien; Dänemark; Estland; Finnland; Frankreich; Deutschland; Griechenland; Ungarn; Island; Irland; Israel; Italien; Japan; Republik Korea; Lettland; Litauen; Luxemburg; Mexiko; Niederlande; Neuseeland; Norwegen; Polen; Portugal; Slowakei; Slowenien; Spanien; Schweden; Schweiz; Türkiye; Vereinigtes Königreich; Vereinigte Staaten.

6.1 Einheitliche OECD-Basisklauseln

Thalassa verarbeitet Kundendaten ausschließlich zur Bereitstellung, Absicherung, Wartung und Abrechnung von Thalassa Assistant und nicht für eigenständige Werbe-, Verkaufs-, Profiling- oder KI-Trainingszwecke.

Soweit ein lokales Recht Begriffe wie Processor, Service Provider, Contractor, Operator, Entrusted Processor oder vergleichbare Rollen verwendet, wird Thalassa funktional in dieser Rolle tätig, soweit der Kunde die Zwecke und Mittel der betreffenden Verarbeitung bestimmt.

Unterauftragsverarbeiter dürfen nur nach den Regeln des Master-AVV eingesetzt werden. Thalassa verpflichtet diese Anbieter vertraglich zu einem im Wesentlichen gleichwertigen Datenschutzniveau.

Betroffenenrechte werden über den Kunden koordiniert, sofern Thalassa nicht nach zwingendem Recht direkt handeln muss.

Datenpannen werden nach den strengeren Vorgaben des Master-AVV und des jeweils zwingenden lokalen Rechts behandelt.

Drittlandübermittlungen erfolgen nur nach den Transferregeln des Master-AVV und der jeweils anwendbaren lokalen Vorschriften.

6.2 EU-/EWR-OECD-Staaten: GDPR-Kern plus nationale Ergänzung

Für die folgenden OECD-Staaten im EU-/EWR-Raum gilt der GDPR-Kern des Master-AVV als primäre Auftragsverarbeitungsregel. Die jeweilige nationale Ergänzung betrifft insbesondere nationale Durchführungsgesetze, Beschäftigtendaten, Berufsgeheimnisse, Bußgeld-/Behördenzuständigkeiten, Telekommunikations-/Cookie-Regeln und sektorale Sondervorschriften.

Land	Lokales Ergänzungsrecht	Länderergänzung
Österreich	DSG und DSGVO-Durchführungsvorschriften	Bei österreichischen Kunden gelten nationale Regeln insbesondere zu Behördenzuständigkeit, Datenschutzgeheimnis, Beschäftigtendaten und besonderen gesetzlichen Aufbewahrungs-/Auskunftspflichten ergänzend.
Belgien	Belgisches Datenschutzgesetz vom 30.07.2018 und DSGVO	Bei belgischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, Sprach-/Informationspflichten, Beschäftigtendaten und straf-/verwaltungsrechtlichen Besonderheiten ergänzend.
Tschechien	Act No. 110/2019 Coll. und DSGVO	Bei tschechischen Kunden gelten nationale Regeln insbesondere zu öffentlichen Stellen, Beschäftigtendaten, Aufsichtsbehörde und besonderen nationalen Rechtsgrundlagen ergänzend.
Dänemark	Danish Data Protection Act und DSGVO	Bei dänischen Kunden gelten nationale Regeln insbesondere zu Beschäftigtendaten, nationalen ID-Nummern, Aufsichtsbehörde und sektoralen Sondervorschriften ergänzend.
Estland	Personal Data Protection Act und DSGVO	Bei estnischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, öffentlichen Stellen, elektronischer Kommunikation und sektoralen Pflichten ergänzend.
Finnland	Data Protection Act 1050/2018 und DSGVO	Bei finnischen Kunden gelten nationale Regeln insbesondere zu Beschäftigtendaten, öffentlichen Registern, Aufsichtsbehörde und sektorspezifischen Pflichten ergänzend.
Frankreich	Loi Informatique et Libertés und	Bei französischen Kunden gelten nationale Regeln

Land	Lokales Ergänzungsrecht	Länderergänzung
	DSGVO	insbesondere zu CNIL-Anforderungen, Beschäftigtendaten, Berufsgeheimnissen, Gesundheitsdaten und Cookies ergänzend.
Deutschland	BDSG, Landesdatenschutzgesetze und DSGVO	Bei deutschen Kunden gelten nationale Regeln insbesondere zu Beschäftigtendaten, Datenschutzbeauftragten, Berufsgeheimnisträgern, Landesrecht und Aufsichtsbehörden ergänzend.
Griechenland	Law 4624/2019 und DSGVO	Bei griechischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, Beschäftigtendaten, öffentlichen Stellen und elektronischer Kommunikation ergänzend.
Ungarn	Info Act CXII of 2011 und DSGVO	Da Thalassa in Ungarn sitzt, gelten ungarische Durchführungsvorschriften ohnehin ergänzend; bei ungarischen Kunden zusätzlich lokale NAIH-/Informationspflichten.
Island	Act No. 90/2018 und EWR-DSGVO	Bei isländischen Kunden gilt die EWR-Umsetzung der DSGVO mit nationalen Ergänzungen zu Aufsichtsbehörde, Beschäftigtendaten und sektoralen Pflichten.
Irland	Data Protection Act 2018 und DSGVO	Bei irischen Kunden gelten nationale Regeln insbesondere zu DPC-Zuständigkeit, Beschäftigtendaten, Kindern, elektronischer Kommunikation und behördlichen Anforderungen ergänzend.
Italien	Codice Privacy, Legislative Decree 196/2003 as amended, und DSGVO	Bei italienischen Kunden gelten nationale Regeln insbesondere zu Garante-Vorgaben, Beschäftigtendaten, Berufsgeheimnissen, Gesundheitsdaten und Marketing/Cookies ergänzend.
Lettland	Personal Data Processing Law und DSGVO	Bei lettischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, öffentlichen Stellen, Beschäftigtendaten und sektorspezifischen Vorschriften ergänzend.
Litauen	Law on Legal Protection of Personal Data und DSGVO	Bei litauischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, Beschäftigtendaten, öffentlichen Stellen und nationalen Verfahren ergänzend.
Luxemburg	Gesetz vom 01.08.2018 und DSGVO	Bei luxemburgischen Kunden gelten nationale Regeln insbesondere zu CNPD-Zuständigkeit, Beschäftigtendaten, Berufsgeheimnissen und Finanz-/Beratungssektor ergänzend.
Niederlande	UAVG und DSGVO	Bei niederländischen Kunden gelten nationale Regeln insbesondere zu AP-Zuständigkeit, BSN/nationalen Kennzeichen, Beschäftigtendaten und sektoralen Sondervorschriften ergänzend.
Norwegen	Personal Data Act und EWR-DSGVO	Bei norwegischen Kunden gilt die EWR-Umsetzung der DSGVO mit nationalen Ergänzungen zu Aufsichtsbehörde, Beschäftigtendaten und elektronischer Kommunikation.
Polen	Polish Data Protection Act 2018 und DSGVO	Bei polnischen Kunden gelten nationale Regeln insbesondere zu UODO-Zuständigkeit, Beschäftigtendaten, öffentlichen Stellen und nationalen Verfahren ergänzend.
Portugal	Law 58/2019 und DSGVO	Bei portugiesischen Kunden gelten nationale Regeln insbesondere zu CNPD-Zuständigkeit, Beschäftigtendaten, Kindern, elektronischer Kommunikation und Aufbewahrung ergänzend.

Land	Lokales Ergänzungsrecht	Länderergänzung
Slowakei	Act No. 18/2018 Coll. und DSGVO	Bei slowakischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, Beschäftigtendaten, öffentlichen Stellen und nationalen Verfahren ergänzend.
Slowenien	ZVOP-2 und DSGVO	Bei slowenischen Kunden gelten nationale Regeln insbesondere zu Aufsichtsbehörde, Video-/Beschäftigtendaten, öffentlichen Stellen und nationalen Verfahren ergänzend.
Spanien	LOPDGDD und DSGVO	Bei spanischen Kunden gelten nationale Regeln insbesondere zu AEPD-Vorgaben, digitalen Rechten, Beschäftigtendaten, Kindern und Cookies ergänzend.
Schweden	Data Protection Act 2018:218 und DSGVO	Bei schwedischen Kunden gelten nationale Regeln insbesondere zu IMY-Zuständigkeit, Beschäftigtendaten, öffentlichen Stellen und sektoralen Vorschriften ergänzend.

6.3 Nicht-EU-/Nicht-EWR-OECD-Staaten: Länderergänzungen

Für die nachstehenden Staaten sind zusätzliche nationale Datenschutzpflichten wahrscheinlicher, weil die DSGVO nicht automatisch das gesamte lokale Regime des Kunden ersetzt. Die Klauseln gelten ergänzend und nur im anwendbaren Umfang.

Australien

Lokale Rechtsgrundlage / Einordnung	Privacy Act 1988, Australian Privacy Principles (APPs) und Notifiable Data Breaches Scheme.
Lokale Einordnung	Der Kunde bleibt für Transparenz, Rechtsgrundlage und APP-konforme Nutzung verantwortlich. Thalassa verarbeitet im Auftrag und nicht für eigene Inhaltszwecke.
Processor-/Service-Provider-Pflichten	Thalassa nutzt Kundendaten nur für die vereinbarten Geschäftszwecke, setzt angemessene Sicherheitsmaßnahmen um und unterstützt den Kunden bei APP-bezogenen Anfragen.
Übermittlung / Zugriff	Soweit Kundendaten aus Australien nach Europa übertragen werden, gelten die vertraglichen Schutzmaßnahmen des Master-AVV. Der Kunde bleibt für seine APP-8-Prüfung verantwortlich.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Auskunfts-/Berichtigungsanfragen und meldet Sicherheitsvorfälle nach dem strengeren Standard aus Master-AVV und lokalem Recht.
Besonderheit für Thalassa Assistant	Meetinginhalte, Audio, Transkripte und Screenshots werden nicht für Profiling, Werbung oder KI-Training verwendet.

Kanada

Lokale Rechtsgrundlage / Einordnung	PIPEDA sowie anwendbare provinzielle Privatsektor-Gesetze, insbesondere Quebec, Alberta und British Columbia, soweit einschlägig.
Lokale Einordnung	Der Kunde bleibt accountable organisation/controller im lokalen Sinn. Thalassa handelt als Dienstleister/Processor für die vom Kunden bestimmten Zwecke.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet Daten nur für die beauftragte Leistung, wahrt Vertraulichkeit, Sicherheitsmaßnahmen, Löschung und Subprocessor-Kontrolle.
Übermittlung / Zugriff	Grenzüberschreitende Verarbeitung in Europa ist offenzulegen, soweit der Kunde hierzu nach lokalem Recht verpflichtet ist. Bei Quebec-Daten

Lokale Rechtsgrundlage / Einordnung	PIPEDA sowie anwendbare provinzielle Privatsektor-Gesetze, insbesondere Quebec, Alberta und British Columbia, soweit einschlägig.
	können zusätzliche Transfer- und Vertragsprüfungen erforderlich sein.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Access-/Correction-Requests und Sicherheitsvorfällen. Meldungen erfolgen an den Kunden so, dass dieser eigene kanadische Meldepflichten erfüllen kann.
Besonderheit für Thalassa Assistant	Für regulierte kanadische Kunden, Gesundheitsdaten, öffentliche Stellen oder Quebec-Law-25-Fälle sollte vor Enterprise-Abschluss eine gesonderte lokale Prüfung erfolgen.

Chile

Lokale Rechtsgrundlage / Einordnung	Law No. 19.628; zusätzlich Law No. 21.719 als reformiertes Datenschutzregime ab dem jeweils geltenden Inkrafttretenszeitpunkt.
Lokale Einordnung	Bis zum Inkrafttreten der neuen Regelungen bleiben bestehende chilenische Vorschriften maßgeblich; danach gelten die verschärften Pflichten ergänzend.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet nur im Rahmen der Kundenweisung, hält Sicherheitsmaßnahmen ein und nutzt Kundendaten nicht für eigene Sekundärzwecke.
Übermittlung / Zugriff	Internationale Übermittlungen erfolgen nach Master-AVV, SCC bzw. gleichwertigen Schutzmaßnahmen, soweit lokales Recht dies verlangt.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei ARCO-/Betroffenenrechten und Vorfällen im Rahmen der technischen Möglichkeiten.
Besonderheit für Thalassa Assistant	Für chilenische Kunden ist wegen des Rechtsübergangs eine erneute Prüfung der Anlage erforderlich, sobald Law No. 21.719 vollständig gilt.

Kolumbien

Lokale Rechtsgrundlage / Einordnung	Law 1581 of 2012, Decree 1377 of 2013 und einschlägige SIC-Vorgaben.
Lokale Einordnung	Der Kunde bleibt Responsable del Tratamiento; Thalassa handelt als Encargado del Tratamiento, soweit sie personenbezogene Daten im Auftrag verarbeitet.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet nur nach Weisung, wahrt Vertraulichkeit und trifft Sicherheitsmaßnahmen gegen unbefugten Zugriff, Verlust, Änderung oder Offenlegung.
Übermittlung / Zugriff	Übermittlungen nach Europa erfolgen im Rahmen der vertraglichen Schutzmaßnahmen und soweit erforderlich auf Basis von Autorisierung, Vertrag oder anderer zulässiger Grundlage.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt den Kunden bei consulta-/reclamo-Prozessen und bei Sicherheitsvorfällen.
Besonderheit für Thalassa Assistant	Kundendaten werden nicht verkauft, nicht für Thalassa-eigenes KI-Training genutzt und nicht außerhalb der direkten Dienstleistung verwendet.

Costa Rica

Lokale Rechtsgrundlage / Einordnung	Law No. 8968 on Protection of the Person regarding the Processing of Personal Data und ergänzende Vorschriften.
Lokale Einordnung	Der Kunde bleibt für Einwilligung, Information und Zweckbindung verantwortlich. Thalassa agiert als Dienstleister im Auftrag.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet Daten nur zweckgebunden, vertraulich und mit angemessenen Sicherheitsmaßnahmen.
Übermittlung / Zugriff	Internationale Verarbeitung in Europa erfolgt nach den vertraglichen Regeln des Master-AVV und nach den Anforderungen des anwendbaren costa-ricanischen Rechts.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Auskunft, Berichtigung, Löschung und Widerspruch im Rahmen der technischen Möglichkeiten.
Besonderheit für Thalassa Assistant	Für besondere Datenkategorien oder Minderjährige ist eine gesonderte lokale Rechtmäßigkeitsprüfung durch den Kunden erforderlich.

Israel

Lokale Rechtsgrundlage / Einordnung	Protection of Privacy Law, 1981, Protection of Privacy Regulations und anwendbare Authority-Guidance.
Lokale Einordnung	Der Kunde bleibt Database Owner/Controller im lokalen Sinn; Thalassa handelt als Outsourcing-/Processing-Dienstleister für die vereinbarten Zwecke.
Processor-/Service-Provider-Pflichten	Thalassa hält angemessene Sicherheits-, Vertraulichkeits- und Subprocessor-Pflichten ein und verarbeitet Kundendaten nicht für eigene Zwecke.
Übermittlung / Zugriff	Übermittlungen nach Europa erfolgen nach Master-AVV und unter Beachtung der israelischen Regeln für Datenübermittlungen ins Ausland.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Betroffenenrechten und Sicherheitsvorfällen, soweit technisch möglich und vertraglich erforderlich.
Besonderheit für Thalassa Assistant	Für israelische Datenbanken mit Registrierungs-, Sicherheitslevel- oder Outsourcing-Anforderungen können zusätzliche kundenseitige Dokumentationspflichten bestehen.

Japan

Lokale Rechtsgrundlage / Einordnung	Act on the Protection of Personal Information (APPI) und Vorgaben der Personal Information Protection Commission.
Lokale Einordnung	Der Kunde bleibt Business Operator/Controller; Thalassa verarbeitet als entrustierter Dienstleister für die beauftragten Zwecke.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet Daten nicht über den Umfang der Entrustment-Beziehung hinaus, schützt Vertraulichkeit und kontrolliert Subprocessor.
Übermittlung / Zugriff	Übermittlungen zwischen Japan und EU/EWR können durch anwendbare Angemessenheits-/Transfermechanismen erleichtert sein; zusätzliche Informationen oder Einwilligungen bleiben Sache des Kunden, soweit erforderlich.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Offenlegung, Korrektur, Nutzungsstopp und Vorfallbearbeitung nach APPI im technisch möglichen Umfang.
Besonderheit für Thalassa Assistant	KI-Training, Werbung, Profiling und Zweckänderungen mit Kundendaten

Lokale Rechtsgrundlage / Einordnung	Act on the Protection of Personal Information (APPI) und Vorgaben der Personal Information Protection Commission.
	sind ausgeschlossen, sofern der Kunde nicht gesondert rechtmäßig anweist.

Republik Korea

Lokale Rechtsgrundlage / Einordnung	Personal Information Protection Act (PIPA) und Vorgaben der Personal Information Protection Commission.
Lokale Einordnung	Der Kunde bleibt Personal Information Controller; Thalassa handelt als Outsourced Processor/Consignee im Rahmen der Kundenweisung.
Processor-/Service-Provider-Pflichten	Thalassa wahrt Zweckbindung, technische und organisatorische Sicherheit, Subprocessor-Kontrolle und Vertraulichkeit.
Übermittlung / Zugriff	Internationale Übermittlungen nach Europa erfolgen nach Master-AVV und den koreanischen Anforderungen an grenzüberschreitende Verarbeitung/Outsourcing, soweit anwendbar.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Data-Subject-Requests und Vorfallmeldungen mit den erforderlichen Informationen über Art, Umfang und Maßnahmen.
Besonderheit für Thalassa Assistant	Für koreanische Nutzerinformationen, Kinder oder sensible Daten sind gesonderte Informations-/Einwilligungspflichten durch den Kunden zu prüfen.

Mexiko

Lokale Rechtsgrundlage / Einordnung	Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP), Regulations und anwendbare behördliche Vorgaben.
Lokale Einordnung	Der Kunde bleibt Responsable; Thalassa handelt als Encargado für die vertraglich definierten Zwecke.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet nur nach Kundenweisung, bewahrt Vertraulichkeit, setzt Sicherheitsmaßnahmen um und gibt Daten nicht an Dritte weiter, außer an genehmigte Subprocessor.
Übermittlung / Zugriff	Internationale Verarbeitung in Europa erfolgt auf Grundlage des Master-AVV und der lokalen Transferanforderungen, soweit anwendbar.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei ARCO-Rechten und Sicherheitsvorfällen im technisch möglichen Umfang.
Besonderheit für Thalassa Assistant	Kundendaten werden nicht verkauft, nicht geteilt für Werbung und nicht für Thalassa-eigene KI-Modelle genutzt.

Neuseeland

Lokale Rechtsgrundlage / Einordnung	Privacy Act 2020, Information Privacy Principles und Notifiable Privacy Breach-Regime.
Lokale Einordnung	Der Kunde bleibt Agency/Controller im lokalen Sinn. Thalassa agiert als Dienstleister für die beauftragte Verarbeitung.
Processor-/Service-Provider-Pflichten	Thalassa nutzt Daten nur zur Serviceerbringung, schützt sie angemessen und beschränkt Subprocessor nach Master-AVV.
Übermittlung / Zugriff	Grenzüberschreitende Verarbeitung in Europa erfolgt nach den Schutzmaßnahmen des Master-AVV. Der Kunde bleibt für seine IPP-12-Beurteilung verantwortlich.

Lokale Rechtsgrundlage / Einordnung	Privacy Act 2020, Information Privacy Principles und Notifiable Privacy Breach-Regime.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Access-/Correction-Requests und meldet relevante Privacy Breaches an den Kunden.
Besonderheit für Thalassa Assistant	Thalassa führt keine Voiceprint-Erstellung, keine biometrische Identifikation und kein KI-Training mit Kundendaten durch.

Schweiz

Lokale Rechtsgrundlage / Einordnung	Bundesgesetz über den Datenschutz (DSG/FADP) und Verordnung über den Datenschutz.
Lokale Einordnung	Der Kunde bleibt Verantwortlicher im Sinn des Schweizer DSG; Thalassa handelt als Auftragsbearbeiterin, soweit sie im Auftrag verarbeitet.
Processor-/Service-Provider-Pflichten	Die bereits vorhandene Schweizer Ergänzung im Master-AVV bleibt vorrangig. Diese Länderklausel bestätigt zusätzlich Zweckbindung, Vertraulichkeit und Subprocessor-Kontrolle.
Übermittlung / Zugriff	Übermittlungen in die EU/EWR gelten grundsätzlich als Übermittlungen in angemessene Staaten. Für andere Drittländer sind SCC oder gleichwertige Garantien zu verwenden.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Auskunfts-, Lösch- und Berichtigungsrechten sowie bei Sicherheitsvorfällen.
Besonderheit für Thalassa Assistant	Für besonders schützenswerte Personendaten, Profiling mit hohem Risiko oder schweizerische Berufsgeheimnisse ist eine gesonderte Kundenprüfung erforderlich.

Türkiye

Lokale Rechtsgrundlage / Einordnung	Law No. 6698 on the Protection of Personal Data (KVKK) und einschlägige Beschlüsse/Leitlinien der KVKK-Behörde.
Lokale Einordnung	Der Kunde bleibt Data Controller; Thalassa handelt als Data Processor/Service Provider im Rahmen der Kundenweisung.
Processor-/Service-Provider-Pflichten	Thalassa verarbeitet nur zweckgebunden, trifft Sicherheitsmaßnahmen, wahrt Vertraulichkeit und beschränkt Subprocessor.
Übermittlung / Zugriff	Internationale Übermittlungen nach Europa erfordern die vom türkischen Recht vorgesehenen Grundlagen, soweit KVKK anwendbar ist.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Betroffenenrechten und Sicherheitsvorfällen, soweit technisch möglich und gesetzlich erforderlich.
Besonderheit für Thalassa Assistant	Für türkische Kunden können zusätzliche Informations-, Einwilligungs-, Registrierung- oder Transferpflichten bestehen; diese sind vor breitem Launch gesondert zu prüfen.

Vereinigtes Königreich

Lokale Rechtsgrundlage / Einordnung	UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations und ICO-Guidance.
Lokale Einordnung	Der Kunde bleibt Controller oder Processor; Thalassa handelt als Processor oder Subprocessor entsprechend der tatsächlichen Rollenverteilung.
Processor-/Service-Provider-Pflichten	Die bereits vorhandene UK-Ergänzung im Master-AVV bleibt vorrangig.

Lokale Rechtsgrundlage / Einordnung	UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations und ICO-Guidance.
	Diese Länderklausel bestätigt zusätzlich Weisungsbindung, Security, Subprocessor-Kontrolle und kein KI-Training.
Übermittlung / Zugriff	UK-to-EEA-Transfers sind nach der jeweils geltenden britischen Adequacy-Regel grundsätzlich erleichtert; sonst sind IDTA oder UK Addendum zu verwenden.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei UK-GDPR-Rechten, DPIA/TRA-Anforderungen und Personal Data Breaches.
Besonderheit für Thalassa Assistant	Für britische Education-, Employment-, Financial-Services- oder Legal-Kunden sollte bei Enterprise-Nutzung eine sektorale Prüfung erfolgen.

Vereinigte Staaten

Lokale Rechtsgrundlage / Einordnung	U.S. State Privacy Laws, insbesondere CCPA/CPRA und weitere anwendbare State Consumer Privacy Acts; sektoral zusätzlich z. B. HIPAA/GLBA/FERPA nur bei ausdrücklicher Vereinbarung.
Lokale Einordnung	Der Kunde bleibt Business/Controller. Thalassa handelt als Service Provider, Contractor, Processor oder Subprocessor, soweit das jeweilige State Law dies vorsieht.
Processor-/Service-Provider-Pflichten	Die bereits vorhandene USA-Ergänzung im Master-AVV bleibt vorrangig. Kundendaten werden nicht verkauft, nicht für cross-context behavioral advertising geteilt, nicht für eigene KI-Modelle trainiert und nicht außerhalb der direkten Geschäftsbeziehung genutzt.
Übermittlung / Zugriff	Datenverarbeitung in Europa erfolgt nach Master-AVV. Zugriff durch US-Subprocessor wie Deepgram ist nur nach DPA, SCC/DPF oder sonstiger zulässiger Transfergrundlage und mit deaktivierter Sekundärnutzung zulässig.
Betroffenenrechte / Sicherheitsvorfälle	Thalassa unterstützt bei Consumer Requests, Security Incidents und Nachweispflichten nach den anwendbaren State Laws.
Besonderheit für Thalassa Assistant	HIPAA-, GLBA-, FERPA- oder arbeitsrechtlich regulierte US-Daten dürfen nur verarbeitet werden, wenn die erforderlichen Zusatzverträge und Produktkonfigurationen ausdrücklich abgeschlossen wurden.

6.4 Implementierungscheckliste für die Website / Signaturstrecke

Beim B2B-Checkout muss das Land der Kundenniederlassung erfasst werden; IP-Geolocation allein reicht nicht als Vertragsgrundlage.

Der Kunde muss bestätigen, ob er als Controller oder als Processor für Dritte handelt. Falls Processor: Thalassa ist Subprocessor.

Der Kunde muss bestätigen, dass die unterzeichnende Person vertretungsberechtigt ist.

Der akzeptierte Master-AVV muss mit Versionsnummer, OECD-Anlage, Zeitstempel, Account-ID und Dokument-Hash protokolliert werden.

Für regulierte Branchen sollte ein Enterprise-Flag gesetzt werden, damit zusätzliche lokale Prüfung ausgelöst wird.

Für B2C-Nutzer darf diese AVV nicht als Datenschutzhinweis verwendet werden. Dort sind Terms of Service, Privacy Policy, Cookie/Tracking-Hinweise und Minderjährigenregeln separat erforderlich.