Auftragsverarbeitungsvertrag mit Verschwiegenheitsverpflichtung

Version 2.1 · Stand: 17. November 2026

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO mit Verschwiegenheitsverpflichtung nach § 62a StBerG und § 203 StGB

zwischen

dem **Kunden**, dem Inhaber eines Ora-Kontos, der Ora für berufliche oder geschäftliche Zwecke nutzt, nachfolgend „**Verantwortlicher**“,

und

Gianmarco Colaiacolo, Einzelunternehmer, handelnd unter „Ora“, Roman-Herzog-Str. 26, 81248 München, Deutschland, E-Mail support@ora-ai.de, nachfolgend „**Auftragsverarbeiter**“.

1. Gegenstand, Abschluss und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen bei der Nutzung von Ora (Mac-App „Ora“, Ora-Dienst api.ora-ai.de) für berufliche oder geschäftliche Zwecke.

(2) Der Vertrag wird in Textform geschlossen (Art. 28 Abs. 9 DSGVO, § 62a Abs. 3 StBerG). Er wird mit der Registrierung, bei der der Verantwortliche seine Kenntnisnahme bestätigt, Bestandteil des Nutzungsvertrags und gilt, sobald und soweit der Verantwortliche Ora beruflich oder geschäftlich nutzt. Der Auftragsverarbeiter speichert Zeitpunkt und Version der Bestätigung am Konto und stellt auf Wunsch eine unterzeichnete Ausfertigung bereit.

(3) Der Vertrag gilt für die Dauer des Nutzungsvertrags und endet mit dessen Beendigung oder der Löschung des Kontos.

2. Art und Zweck der Verarbeitung, Datenarten, Betroffene

(1) **Art und Zweck:** Der Auftragsverarbeiter nimmt über den Ora-Dienst Audio und Text entgegen, leitet sie zur Spracherkennung und zur KI-Verarbeitung (Aufbereiten, Zusammenfassen, Beantworten von Fragen und weitere vom Verantwortlichen gewählte Funktionen) an die Unterauftragsverarbeiter nach Anlage 1 weiter und gibt das Ergebnis an die App zurück. Auf Wunsch des Verantwortlichen legt er außerdem verschlüsselte Inhalte für die Synchronisierung zwischen dessen Geräten ab.

(2) **Datenarten:** Inhalte von Diktaten und Meetings:

- Audio (Modus Schnell; bei Meetings laufend und nach dem Ende als ganze Aufnahme beider Spuren; die Unterscheidung der Sprecher übernimmt der Unterauftragsverarbeiter innerhalb der Verbindung bzw. über die ganze Aufnahme, der Auftragsverarbeiter übermittelt keine Stimmproben und bildet keine Stimmprofile),
- Text, Anweisung der Vorlage, passende eigene Begriffe, bis zu 100 Begriffe als Kontext der Spracherkennung (bei Meetings bis zu 300 Begriffe aus eigenen Begriffen und Grundvokabular, das Fachgebiet des Profils sowie bis zu 30 Anzeigenamen von Teilnehmern, soweit der Verantwortliche das nicht ausschaltet),
- bei Funktionen, die der Verantwortliche wählt: Text um den Cursor und Markierung, Fenster- und Bildschirmtext und daraus gewonnene Namen, zu überarbeitender Text mit Anweisung (Feinschliff), Mitschrift eines Meetings oder Ausschnitte aus mehreren Meetings mit Fragen (Chat), Zusammenfassung für ein Follow-up, Anzeigenamen von Sprechern, Ausschnitt zur Erkennung des Meeting-Endes, einzelne Wörter zur Wortprüfung,
- bei Synchronisierung: verschlüsselte Inhalte und Metadaten (Bereich, Größe, Zeitpunkte, Kennungen).

Die Inhalte können personenbezogene Daten aller Art enthalten, auch besondere Kategorien nach Art. 9 DSGVO und Informationen, die einem Berufsgeheimnis unterliegen.

(3) **Betroffene:** der Verantwortliche, seine Beschäftigten, in Diktaten genannte Personen (zum Beispiel Mandanten, Kunden, Patienten, Geschäftspartner) und Teilnehmer mitgeschriebener Meetings, einschließlich ihrer Stimme.

(4) **Speicherung:** Der Ora-Dienst ist so gestaltet, dass er Inhalte nur durchleitet und im Arbeitsspeicher verarbeitet, solange die Anfrage läuft, und sie nicht dauerhaft speichert. Ausnahme ist die Synchronisierung: Dort legt er die vom Verantwortlichen auf dessen Geräten verschlüsselten Inhalte als Chiffre ab; der Dienst ist so gestaltet, dass der Auftragsverarbeiter sie nicht lesen kann. Audio für die Auswertung eines Meetings im Modus Schnell hält die App höchstens 24 Stunden nach dem Ende des Meetings verschlüsselt auf dem Gerät des Verantwortlichen und sendet es nach dem Meeting in den privaten Dateispeicher des Ora-Dienstes (Anlage 1). Dort und beim Unterauftragsverarbeiter für die Spracherkennung liegt es nur bis zur Löschung nach dem Ergebnis, spätestens 24 Stunden nach dem Start der Auswertung. Der Ora-Dienst ist so gestaltet, dass er die Aufnahme nur zur Weiterleitung nutzt. Unterauftragsverarbeiter verarbeiten Inhalte nach Anlage 1 in dessen Auftrag; deren Speicherung richtet sich nach den mit ihnen geschlossenen Verträgen.

(5) Nicht Gegenstand sind die Konto-, Geräte- und Zählerdaten, für die der Auftragsverarbeiter eigener Verantwortlicher ist (siehe Datenschutzerklärung), und Daten, die nur auf dem Gerät des Verantwortlichen verarbeitet werden und den Auftragsverarbeiter nicht erreichen.

3. Weisungen

(1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Drittlandübermittlungen, es sei denn, er ist durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; er teilt dies dem Verantwortlichen vorher mit, sofern das Recht es nicht verbietet.

(2) Die Weisungen ergeben sich aus diesem Vertrag und den Einstellungen in der App (insbesondere Modus Schnell oder Lokal, KI-Aufbereitung, Meeting-Mitschrift, optionale Funktionen und Synchronisierung). Weitere Weisungen erteilt der Verantwortliche in Textform an support@ora-ai.de.

(3) Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, weist er unverzüglich darauf hin.

4. Vertraulichkeit und Verschwiegenheit

(1) Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Unterliegt der Verantwortliche einer beruflichen Verschwiegenheitspflicht, insbesondere nach § 203 StGB oder § 57 Abs. 1 StBerG, gilt zusätzlich:

1. Der Auftragsverarbeiter ist zur Verschwiegenheit über alle fremden Geheimnisse verpflichtet, die ihm bei der Leistung bekannt werden.
2. Er verschafft sich Kenntnis von fremden Geheimnissen nur, soweit die Leistung es erfordert, und nutzt sie zu keinem anderen Zweck.
3. Er wurde darauf hingewiesen, dass er als mitwirkende Person nach § 203 Abs. 4 StGB strafbar sein kann, wenn er ein fremdes Geheimnis unbefugt offenbart.
4. Weitere Personen und Unterauftragsverarbeiter verpflichtet er zur Verschwiegenheit und weist sie auf die Strafbarkeit nach § 203 Abs. 4 StGB hin, soweit dies gesetzlich erforderlich und vertraglich möglich ist (§ 62a Abs. 3 StBerG). Gegenüber Unterauftragsverarbeitern legt er im Übrigen die Pflichten nach Nr. 6 Abs. 3 vertraglich auf.

(3) Ob der Einsatz der Unterauftragsverarbeiter nach Anlage 1 den berufsrechtlichen Anforderungen des Verantwortlichen genügt, insbesondere § 62a Abs. 4 StBerG bei Leistungen im Ausland, prüft der Verantwortliche selbst. Der Auftragsverarbeiter stellt dafür die Angaben in den Anlagen bereit.

5. Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach **Anlage 2** (Art. 32 DSGVO) und darf sie anpassen, sofern das Schutzniveau nicht unterschritten wird.

6. Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern. Die bei Vertragsschluss eingesetzten stehen in **Anlage 1**.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage im Voraus per E-Mail an die im Konto hinterlegte Adresse oder in der App über jede beabsichtigte Hinzuziehung oder Ersetzung. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. In diesem Fall kann er die berufliche oder geschäftliche Nutzung beenden und sein Konto löschen.

(3) Der Auftragsverarbeiter legt jedem Unterauftragsverarbeiter vertraglich im Wesentlichen dieselben Datenschutzpflichten auf wie in diesem Vertrag. Kommt dieser seinen Pflichten nicht nach, haftet der Auftragsverarbeiter dem Verantwortlichen für deren Erfüllung nach Maßgabe von Nr. 12.

7. Drittländer

(1) Der Auftragsverarbeiter hat die Dienste so eingerichtet, dass Inhalte in Rechenzentren in der Europäischen Union verarbeitet werden (Anlage 1).

(2) Haben Unterauftragsverarbeiter ihren Sitz außerhalb der EU oder ist ein Zugriff von dort möglich, erfolgt die Übermittlung nur unter den Voraussetzungen der Art. 44 ff. DSGVO, auf Grundlage der Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO) und, soweit der Anbieter unter dem EU-US Data Privacy Framework zertifiziert ist, des Angemessenheitsbeschlusses (Art. 45 DSGVO).

8. Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei Anträgen betroffener Personen (Art. 12 bis 22 DSGVO). Da er Inhalte nicht dauerhaft speichert, kann er zu ihnen in der Regel keine Auskunft erteilen; zur Auswertung von Meeting-Aufnahmen führt er ein Auftragsbuch ohne Inhalte (Anlage 2), aus dem er auf Anfrage Auskunft gibt. Wendet sich eine betroffene Person an ihn, leitet er die Anfrage unverzüglich weiter.

(2) Er unterstützt den Verantwortlichen bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation), soweit es die Art der Verarbeitung und die ihm verfügbaren Informationen zulassen.

9. Meldung von Verletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten, die dessen Daten betrifft, unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, per E-Mail an die im Konto hinterlegte Adresse, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar; fehlende Angaben reicht er nach.

10. Nachweise und Überprüfungen

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die erforderlichen Informationen zum Nachweis der Pflichten nach Art. 28 DSGVO bereit und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer. Sie sind mit angemessener Frist, in der Regel mindestens 14 Tagen, anzukündigen, finden zu üblichen Geschäftszeiten ohne unverhältnismäßige Störung des Betriebs statt und erfolgen vorrangig durch schriftliche Auskünfte und Unterlagen.

11. Löschung und Rückgabe

(1) Inhalte werden nicht dauerhaft gespeichert (Nr. 2 Abs. 4); nach Ende der Verarbeitung sind sie daher in der Regel weder zurückzugeben noch zu löschen. Aufnahmen von Meetings löscht der Auftragsverarbeiter im Dateispeicher und beim Unterauftragsverarbeiter direkt nach dem Ergebnis, bei Fehlern, auf Veranlassung des Verantwortlichen („Verwerfen“, „Löschen“, Abmelden des Geräts) und mit der Löschung des Kontos, sonst durch einen laufenden Aufräumlauf spätestens 24 Stunden nach dem Start der Auswertung. Bei der Synchronisierung löscht der Auftragsverarbeiter die Cloud-Daten auf Veranlassung des Verantwortlichen („Cloud-Daten löschen“) und mit Vertragsende bzw. Löschung des Kontos. Als Rückgabe dient der Export in der App.

(2) Die in Nr. 2 Abs. 5 genannten Daten löscht der Auftragsverarbeiter nach den Fristen der Datenschutzerklärung, bei Löschung des Kontos sofort. Daten, die nur auf dem Gerät des Verantwortlichen liegen, löscht dieser selbst in der App oder durch Deinstallation. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

12. Haftung und Schlussbestimmungen

(1) Gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregeln der Nutzungsbedingungen.

(2) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes vor.

(3) Änderungen dieses Vertrags kündigt der Auftragsverarbeiter mindestens 30 Tage vor Inkrafttreten in Textform an; Abschnitt 12 der Nutzungsbedingungen gilt entsprechend.

(4) Es gilt deutsches Recht. Ist der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist Gerichtsstand München.

Anlage 1: Unterauftragsverarbeiter

Grundlage für Drittlandbezüge ist Nr. 7 Abs. 2. Die Unterauftragsverarbeiter verarbeiten die Daten im Auftrag und nach den Weisungen des Auftragsverarbeiters.

Unterauftragsverarbeiter	Leistung	Sitz	Verarbeitungsort	Daten
Soniox Inc., 1045 Helm Lane, Foster City, CA 94404	Spracherkennung im Modus Schnell (Diktate, Meetings, Unterscheidung der Sprecher), Auswertung der ganzen Meeting-Aufnahme als Auftrag	USA	Region EU; nach Angaben des Anbieters Unterauftragnehmer Amazon Web Services, Google Cloud, Oracle Cloud (EU-Regionen) und Cloudflare	Audio, Sprache, bis zu 100 Begriffe als Kontext (bei Meetings bis zu 300 Begriffe und Anzeigenamen von Teilnehmern); bei der Meeting-Aufnahme Datei oder Abruf-Adresse, Mitschrift und Kontext bis zur Löschung durch den Auftragsverarbeiter, höchstens 24 Stunden nach dem Start der Auswertung
Mistral AI SAS	KI-Aufbereitung, Zusammenfassung, Fragen an Meetings, Feinschliff, weitere gewählte KI-Funktionen, Rückfall bei der Spracherkennung	Frankreich	EU, EU-Endpunkt	Text, Anweisungen, passende Begriffe, gewählter Kontext, Audio im Rückfall

Unteraufragsverarbeiter	Leistung	Sitz	Verarbeitungsort	Daten
Vercel Inc.	Betrieb des Ora-Dienstes und des Konto-Bereichs	USA	Frankfurt am Main	Inhalte im Durchlauf (bei der Meeting-Auswertung die Aufnahme als Strom, nicht gespeichert), technische Verbindungsdaten
Supabase Pte. Ltd.	Konto-Datenbank, Anmeldung, Dateispeicher (App-Updates, Synchronisierung, Meeting-Aufnahmen bis zur Auswertung)	Singapur	Frankfurt am Main	Konto-, Geräte- und Zählerdaten; bei Synchronisierung verschlüsselte Inhalte und Metadaten; Meeting-Aufnahmen höchstens 24 Stunden und Auftragsbuch ohne Inhalte
Sendinblue SAS (Brevo)	Versand von Anmeldelinks und Hinweis-Mails	Frankreich	EU	E-Mail-Adresse
Cloudflare, Inc.	Turnstile, Schutz vor automatisierten Anfragen	USA	weltweites Netz	IP-Adresse, Browserangaben

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Bereich	Maßnahme
Inhalte	Der Ora-Dienst ist so gestaltet, dass er Audio und Text von Diktaten und Meetings nur im Arbeitsspeicher verarbeitet, solange die Anfrage läuft, und nicht in Datenbanken, Dateien, Protokollen oder Fehlerberichten ablegt. Ausnahmen: Synchronisierung und die Aufnahme eines Meetings im Modus Schnell bis zur Auswertung (Nr. 2 Abs. 4).
Übertragung	Verbindungen zwischen App, Ora-Dienst, Konto-Bereich und Unterauftragsverarbeitern laufen über HTTPS bzw. WSS mit TLS 1.2 oder höher; der Konto-Bereich sendet Sicherheits-Header (unter anderem Strict-Transport-Security).
Standort	Ora-Dienst und Konto-Bereich laufen in der Region Frankfurt am Main, die Datenbank und der Dateispeicher in Frankfurt am Main; Mistral und Soniox werden über ihre EU-Endpunkte angesprochen, Meeting-Aufnahmen verarbeitet Soniox in der Region EU.
Datenminimierung	An Unterauftragsverarbeiter gehen nur die für die Anfrage nötigen Inhalte. Vorgesehen ist, dass nicht übermittelt werden: E-Mail-Adresse, Konto-, Geräte- oder Installations-Kennung, IP-Adresse, Kopfzeilen der App, Text von Textbausteinen, Grundvokabular (außer als Kontext bei Meetings, Nr. 2 Abs. 2), Notizen und Titel. Zur Meeting-Auswertung erhält der Unterauftragsverarbeiter als Kennung nur eine zufällige Auftragskennung, nie die Meeting-Kennung. Namen vom Bildschirm gehen höchstens als einzelne Begriffe mit. Es werden keine Geräte- oder Computernamen gespeichert.
Zugangsschutz	Nur angemeldete Geräte können den Ora-Dienst nutzen. Der Geräte-Token ist zufällig, liegt in der Keychain des Geräts (nicht synchronisiert) und beim Dienst nur als SHA-256-Hash. Die App meldet sich über den Browser mit Prüfwert (PKCE) und Einmal-Code an, von denen nur Hashwerte gespeichert werden.
Schlüssel	Der Zugangsschlüssel zu den KI-Diensten liegt als Server-Geheimnis beim Ora-Dienst und nicht in der App.

Bereich	Maßnahme
Zugriffskontrolle	Nutzer können nur ihren eigenen Konto-Datensatz lesen (Anwendung und Row Level Security in der Datenbank). Änderungen an Konto-, Geräte- und Zählerdaten nimmt nur der Server vor. Auswertungsaufträge für Meeting-Aufnahmen sind an Konto und Gerät des ersten Anlegens gebunden; fremde Kennungen erhalten dieselbe Antwort „nicht gefunden“.
Eingabekontrolle	Anfragen werden serverseitig geprüft; angenommen werden nur erlaubte Modelle, Felder und Größen.
Missbrauchsschutz	Anfragen werden je Gerät, Konto, E-Mail-Adresse, IP-Adresse und Installation begrenzt, auch bei Empfehlungscodes. Die Zähler enthalten nur Fingerabdrücke (HMAC) und werden nach höchstens 2 Stunden gelöscht. Anmeldung und Kontaktformular sind durch Cloudflare Turnstile geschützt.
Protokollierung	Betriebsprotokolle enthalten je Anfrage Zeitpunkt, Art, Ergebnis-Code, Dauer, Länge bzw. Audiodauer und eine nicht rückführbare Gerätekurzkennung, ohne Inhalte, Token und IP-Adressen (so vorgesehen); Aufbewahrung 14 Tage, keine Weitergabe an externe Protokolldienste. Zur Meeting-Auswertung führt der Auftragsverarbeiter ein Auftragsbuch als Löschnachweis (zufällige Auftragskennung, Zeitpunkte, Audiodauer, Löschergebnis je Objekt, nie Audio, Text, Kontext oder Adressen), 30 Tage nach der Löschung entfernt.
Löschfristen	Anmelde-Anfragen: Ablauf nach 10 Minuten, Löschung spätestens 2 Stunden danach; Diktat-Belege 2 Stunden; Meeting-Aufnahmen im Dateispeicher und beim Unterauftragsverarbeiter direkt nach dem Ergebnis, spätestens 24 Stunden nach dem Start der Auswertung; Auftragsbuch 30 Tage nach der Löschung; Minutenzähler der Auswertung 48 Stunden; Missbrauchszähler höchstens 2 Stunden; Empfehlungs-Zuordnungen ohne gewährten Monat 90 Tage; Wortzähler laufende und vier vorherige Wochen; Meeting-Zähler 8 Wochen; Geräte-Anmeldungen bei Abmelden, Ersetzen oder nach 60 Tagen ohne Meldung; nicht bestätigte Registrierungen 24 Stunden; Konto sofort bei Löschung, nach 23 Monaten ohne Aktivität mit Ankündigung 30 Tage vorher.
Daten	Wörterbuch, Verlauf, Meetings, Notizen, Textbausteine und gesammelte Wörter speichert die App auf dem Gerät des Verantwortlichen verschlüsselt (Schlüssel im Schlüsselbund), mit

Bereich	Maßnahme
auf dem Gerät	Dateirechten nur für den Benutzer und ohne Time-Machine-Sicherung. Verlauf und Meetings werden nach der gewählten Frist gelöscht (Verlauf nie, 24 Stunden, 7 oder 30 Tage; Meetings 1, 7 oder 30 Tage). Optionale Funktionen sind aus, bis der Verantwortliche sie wählt. Audio wird nicht auf der Festplatte gespeichert, außer die Aufnahme eines Meetings im Modus Schnell: verschlüsselt (Schlüssel im Schlüsselbund dieses Geräts, nicht synchronisiert), bis zur Auswertung und höchstens 24 Stunden nach dem Ende des Meetings.
Synchronisierung	Inhalte werden auf den Geräten des Verantwortlichen Ende-zu-Ende verschlüsselt, der Schlüssel liegt nicht beim Auftragsverarbeiter. Beim Dienst liegen nur die Chiffre und Metadaten. Löschen durch den Verantwortlichen oder mit dem Konto.
Administrative Zugriffe	Zugriff auf Hosting, Datenbank, Konfiguration und das Betreiber-Dashboard hat nur der Auftragsverarbeiter selbst. Das Dashboard zeigt Konto-, Lizenz-, Geräte- und Zählerdaten, keine Inhalte; Änderungen werden mit Zeit, Konto und Aktion protokolliert (13 Monate).
Verfügbarkeit	Fällt die Aufbereitung aus oder ist der Dienst nicht erreichbar, kann die App den erkannten Text unbearbeitet einfügen; im Modus Schnell kann der Ora-Dienst bei Ausfall des Erkennungsdienstes auf einen weiteren Dienst ausweichen, und die App kann bei fehlender Verbindung lokal erkennen, wenn das Sprachmodell geladen ist. Anfragen an Unterauftragsverarbeiter werden nach fester Zeitgrenze abgebrochen.