Vereinbarung zur Auftragsverarbeitung

nach Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

Stand: 12.10.2026

Zwischen

Auftraggeber (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO)

[Firma]
[Straße, Hausnummer]
[PLZ, Ort]
vertreten durch [Name, Funktion]

— nachfolgend „**Auftraggeber**" —

und

Auftragnehmer (Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO)

NoraNotes.ai UG (haftungsbeschränkt)
Dürerstraße 2
93093 Donaustauf
Registergericht Amtsgericht Regensburg, HRB 22430
vertreten durch die Geschäftsführung: Tim Frauenrath, Marcel Gutthann (jeweils einzelvertretungsberechtigt)

— nachfolgend „**Auftragnehmer**" —

— gemeinsam die „**Parteien**" —

Präambel

Der Auftragnehmer betreibt unter der Bezeichnung **NoraNotes** eine Softwareanwendung zur automatisierten Erstellung von Besprechungsprotokollen. Die Anwendung nimmt Besprechungen auf, erstellt daraus Abschriften und wertet diese mit Verfahren der maschinellen Sprachverarbeitung zu strukturierten Protokollen aus.

Der Auftraggeber nutzt diese Anwendung auf Grundlage des zwischen den Parteien geschlossenen Hauptvertrags. Bei der Nutzung werden personenbezogene Daten verarbeitet, für die der Auftraggeber Verantwortlicher bleibt. Diese Vereinbarung konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO und geht dem Hauptvertrag in Datenschutzfragen vor.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

(1) Gegenstand. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers zum Zweck der Erbringung der im Hauptvertrag vereinbarten Leistungen.

(2) Art und Zweck der Verarbeitung umfassen:

a) Aufzeichnung von Online-Besprechungen durch einen als Teilnehmer sichtbaren Aufzeichnungsdienst sowie Entgegennahme vom Auftraggeber hochgeladener Audioaufnahmen;

b) automatisierte Umwandlung der Audioaufnahmen in Text (Abschrift);

c) automatisierte inhaltliche Auswertung der Abschriften zu strukturierten Protokollpunkten, Aufgaben und Zuständigkeiten mittels großer Sprachmodelle;

d) Erzeugung durchsuchbarer Vektorrepräsentationen (Einbettungen) der Inhalte zum Zweck der semantischen Suche;

e) Beantwortung von Fragen des Auftraggebers zu seinen eigenen Inhalten durch einen dialogbasierten Assistenten;

f) Erzeugung und Versand von Protokolldokumenten im PDF-Format an vom Auftraggeber bestimmte Empfänger;

g) Lesen von Kalenderterminen aus einem vom Auftraggeber verbundenen Kalendersystem zum Zweck der automatischen Terminerkennung;

h) Verwaltung von Benutzerkonten, Arbeitsbereichen und Projekten;

i) Speicherung und Bereitstellung der vorgenannten Ergebnisse.

(3) Dauer. Die Vereinbarung läuft für die Dauer des Hauptvertrags. Sie endet mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten aus § 9 (Löschung und Rückgabe) sowie aus § 4 Abs. 6 (Vertraulichkeit) bestehen darüber hinaus fort.

(4) Ort der Verarbeitung. Die Verarbeitung findet in Mitgliedstaaten der Europäischen Union statt. Eine Übermittlung personenbezogener Daten in Drittländer findet nicht statt.

§ 2 Kategorien betroffener Personen und Datenarten

(1) Kategorien betroffener Personen

- Beschäftigte und Organmitglieder des Auftraggebers,
- Teilnehmer von Besprechungen des Auftraggebers, einschließlich externer Personen (Auftraggeber des Auftraggebers, Planungsbeteiligte, ausführende Unternehmen, Behördenvertreter),
- in Besprechungen namentlich erwähnte Dritte,
- vom Auftraggeber eingepflegte Kontakte.

(2) Kategorien personenbezogener Daten

Kategorie	Beispiele
Stammdaten	Name, Firmenzugehörigkeit, Funktion, Rolle im Projekt
Kontaktdaten	E-Mail-Adresse, Telefonnummer, Anschrift
Kontodaten	Anmeldename, Passwort-Hash, Arbeitsbereichs- und Rollenzuordnung
Audiodaten	Sprachaufnahmen von Besprechungen
Abschriften	Wortlaut des Gesprochenen, Sprecherzuordnung, Zeitmarken
Inhaltsdaten	Protokollpunkte, Aufgaben, Termine, Zuständigkeiten, Anhänge
Kalenderdaten	Termintitel, Zeitpunkt, Teilnehmerliste, Besprechungslink

Kategorie	Beispiele
Metadaten	Zeitpunkte der Verarbeitung, Protokolleinträge, technische Kennungen
Zahlungsdaten	Rechnungsanschrift, Abrechnungszeiträume (Zahlungsdaten selbst beim Zahlungsdienstleister)

(3) Besondere Kategorien. Die planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ist nicht Zweck des Auftrags. Den Parteien ist bewusst, dass in freier Rede gelegentlich Angaben fallen können, die einer solchen Kategorie zuzuordnen sind (etwa Hinweise auf Krankheit bei der Erörterung von Abwesenheiten). Der Auftragnehmer wertet solche Angaben nicht gesondert aus und bildet daraus keine Merkmale. Der Auftraggeber trägt dafür Sorge, dass derartige Inhalte nach Möglichkeit vermieden werden.

(4) Keine biometrische Verarbeitung. Der Auftragnehmer erstellt keine Stimmprofile und verarbeitet keine biometrischen Daten zur eindeutigen Identifizierung im Sinne des Art. 4 Nr. 14 DSGVO.

(5) Keine Verhaltens- oder Leistungskontrolle. Die Anwendung ist nicht darauf ausgelegt und wird vom Auftragnehmer nicht dazu verwendet, das Verhalten oder die Leistung von Beschäftigten des Auftraggebers zu bewerten. Auswertungen auf Personenebene über Besprechungen hinweg werden nicht angeboten. Eine etwaige Mitbestimmungspflicht nach § 87 Abs. 1 Nr. 6 BetrVG beim Auftraggeber bleibt unberührt.

(6) Mitwirkungspflicht des Auftraggebers. Der Auftraggeber stellt sicher, dass die nach anwendbarem Recht erforderlichen Einwilligungen der an einer Besprechung beteiligten Personen vorliegen. Auf § 201 StGB wird hingewiesen: Das Aufzeichnen des nichtöffentlich gesprochenen Wortes ohne Einwilligung aller Beteiligten ist strafbar; die Einholung der Einwilligungen obliegt dem Auftraggeber als Verantwortlichem.

§ 3 Weisungsrecht

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Der Hauptvertrag samt dieser Vereinbarung stellt die Erstweisung dar. Die Nutzung der Anwendungsfunktionen durch berechtigte Nutzer des Auftraggebers gilt als Einzelweisung im Rahmen des Auftrags. Eine Verarbeitung ohne Weisung erfolgt nur, soweit der Auftragnehmer durch das Recht der Union oder eines Mitgliedstaats hierzu verpflichtet ist; in diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung über diese rechtliche Verpflichtung, sofern das betreffende Recht eine solche Information nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen sind in Textform zu erteilen. Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

(4) Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Insbesondere werden Inhaltsdaten des Auftraggebers **nicht zum Training von Modellen der künstlichen Intelligenz verwendet** — weder durch den Auftragnehmer noch durch die in Anlage 1 benannten Unterauftragsverarbeiter. Der Auftragnehmer stellt dies vertraglich sicher und weist es auf Verlangen nach.

(5) Weisungsberechtigte Personen

Seite	Name	Funktion	Kontakt
Auftraggeber	[—]	[—]	[—]
Auftragnehmer	Marcel Gutthann	Geschäftsführer	hello@noranotes.ai

Seite	Name	Funktion	Kontakt
Auftragnehmer (Vertretung)	Tim Frauenrath	Geschäftsführer	hello@noranotes.ai

§ 4 Pflichten des Auftragnehmers

(1) Rechtmäßigkeit. Der Auftragnehmer verarbeitet die Daten nur im Rahmen dieser Vereinbarung und der Weisungen des Auftraggebers.

(2) Technische und organisatorische Maßnahmen. Der Auftragnehmer trifft die in **Anlage 2** beschriebenen Maßnahmen nach Art. 32 DSGVO. Er überprüft sie regelmäßig und passt sie dem Stand der Technik an. Eine Verschlechterung des Schutzniveaus ist unzulässig.

(3) Unterstützungspflichten. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei

a) der Beantwortung von Anträgen betroffener Personen (§ 6),

b) der Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33, 34 DSGVO (§ 7),

c) Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und vorherigen Konsultationen nach Art. 36 DSGVO,

d) der Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers, soweit es die Auftragsverarbeitung betrifft.

(4) Verzeichnis. Der Auftragnehmer führt ein Verzeichnis der im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt es dem Auftraggeber auf Verlangen zur Verfügung.

(5) Datenschutzbeauftragter / Kontaktstelle. Der Auftragnehmer benennt als Kontaktstelle für Datenschutzfragen:

Marcel Gutthann, Geschäftsführer (Vertretung: Tim Frauenrath, Geschäftsführer)
hello@noranotes.ai

Sofern eine Benennungspflicht nach Art. 37 DSGVO bzw. § 38 BDSG besteht, benennt der Auftragnehmer einen Datenschutzbeauftragten und teilt dies dem Auftraggeber mit.

(6) Vertraulichkeit. Der Auftragnehmer verpflichtet alle zur Verarbeitung befugten Personen vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit und unterweist sie in den datenschutzrechtlichen Anforderungen. Die Verpflichtung besteht nach Beendigung der Tätigkeit fort.

(7) Grundsatz der Datenminimierung beim Zugriff. Ein Zugriff von Beschäftigten des Auftragnehmers auf Inhaltsdaten des Auftraggebers erfolgt ausschließlich, soweit dies zur Störungsbeseitigung, zur Erfüllung einer Weisung oder zur Wahrung der Systemsicherheit erforderlich ist.

(8) Berichtigung, Löschung, Einschränkung. Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung von Daten nur nach Weisung des Auftraggebers ein. Die Anwendung stellt dem Auftraggeber hierfür Funktionen zur Verfügung.

§ 5 Unterauftragsverhältnisse

(1) Genehmigte Unterauftragsverarbeiter. Der Auftraggeber erteilt mit Abschluss dieser Vereinbarung seine allgemeine schriftliche Genehmigung zur Beauftragung der in **Anlage 1** aufgeführten Unterauftragsverarbeiter.

(2) Änderungen. Der Auftragnehmer informiert den Auftraggeber mindestens **30 Tage** vor der Beauftragung eines weiteren oder der Ersetzung eines bestehenden Unterauftragsverarbeiters in Textform. Der Auftraggeber kann der Änderung innerhalb von **14 Tagen** ab Zugang aus einem wichtigen datenschutzrechtlichen Grund widersprechen. Kann der Widerspruch nicht ausgeräumt werden, ist der Auftraggeber berechtigt, den Hauptvertrag zum Zeitpunkt der Umstellung außerordentlich zu kündigen; bereits gezahlte Entgelte werden zeitanteilig erstattet.

(3) Vertragliche Weitergabe. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieser Vereinbarung entsprechen, insbesondere auf hinreichende Garantien nach Art. 28 Abs. 4 DSGVO. Er bleibt dem Auftraggeber gegenüber für deren Verhalten verantwortlich.

(4) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt, ohne dass ein Zugriff auf Inhaltsdaten des Auftraggebers erfolgt (etwa Telekommunikations- oder Reinigungsleistungen). Ebenfalls nicht erfasst sind Systeme, die der **Auftraggeber selbst betreibt oder gegenüber denen er selbst Verantwortlicher ist** — insbesondere sein eigener Microsoft-365- oder Google-Workspace-Mandant, aus dem Kalenderdaten gelesen werden.

§ 6 Betroffenenrechte

(1) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich, spätestens innerhalb von **drei Werktagen**, an den Auftraggeber weiter und beantwortet es nicht selbst.

(2) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen nach Art. 15 bis 22 DSGVO. Die Anwendung stellt hierfür Funktionen zur Auskunft, Berichtigung, Löschung und Datenübertragung bereit.

(3) Ist die Unterstützung mit einem Aufwand verbunden, der über die bereitgestellten Funktionen hinausgeht, kann der Auftragnehmer eine angemessene Vergütung verlangen. Er weist den Auftraggeber vor Ausführung darauf hin.

§ 7 Verletzung des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft, **unverzüglich** nach Kenntniserlangung in Textform — jedenfalls so rechtzeitig, dass der Auftraggeber seine Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO erfüllen kann.

(2) Die Meldung enthält, soweit bekannt: Beschreibung der Art der Verletzung, Kategorien und ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Gegenmaßnahmen sowie eine Kontaktstelle für Rückfragen. Fehlende Angaben werden unverzüglich nachgereicht.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und stimmt sich hierzu mit dem Auftraggeber ab.

(4) Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO und Benachrichtigungen betroffener Personen nach Art. 34 DSGVO obliegen dem Auftraggeber.

§ 8 Nachweis- und Kontrollrechte

(1) Der Auftragnehmer weist die Einhaltung der Pflichten aus dieser Vereinbarung auf Verlangen in geeigneter Weise nach, insbesondere durch Vorlage der Anlage 2 in jeweils aktueller Fassung, Auskünfte in Textform sowie sonstige geeignete Nachweise. Dem Kontrollinteresse des Auftraggebers ist zunächst auf diesem Weg zu entsprechen.

(2) Der Auftraggeber ist berechtigt, Kontrollen beim Auftragnehmer durchzuführen. Reguläre Kontrollen erfolgen nach Ankündigung mit einer Frist von mindestens **vier Wochen**, während der üblichen Geschäftszeiten, ohne vermeidbare Störung des Betriebsablaufs und höchstens einmal jährlich; dem Kontrollinteresse ist zunächst durch Nachweise nach Absatz 1 zu entsprechen, soweit diese ausreichen. Unberührt bleiben anlassbezogene Kontrollen bei einer Verletzung nach § 7, bei begründetem Verdacht eines Verstoßes gegen diese Vereinbarung oder auf Verlangen einer Aufsichtsbehörde. Die Kosten einer Kontrolle trägt der Auftraggeber; dies gilt nicht für anlassbezogene Kontrollen aufgrund einer vom Auftragnehmer zu vertretenden Verletzung.

(3) Der Auftraggeber kann die Kontrolle durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Der Prüfer darf kein Wettbewerber des Auftragnehmers sein.

(4) Der Auftragnehmer duldet Kontrollen der zuständigen Aufsichtsbehörde und unterstützt diese.

(5) Auskunft zu Prüfungen. Der Auftragnehmer erteilt dem Auftraggeber auf Verlangen Auskunft über Art, Umfang und Turnus der von ihm veranlassten Sicherheitsprüfungen.

§ 9 Löschung und Rückgabe

(1) Nach Beendigung des Hauptvertrags löscht der Auftragnehmer alle im Auftrag verarbeiteten personenbezogenen Daten oder gibt sie nach Wahl des Auftraggebers zurück.

(2) Der Auftraggeber teilt seine Wahl innerhalb von **30 Tagen** nach Vertragsende mit. Trifft er keine Wahl, erfolgt die Löschung.

(3) Für die Datenrückgabe stellt der Auftragnehmer die Inhalte in einem gängigen, maschinenlesbaren Format bereit. Die Bereitstellung erfolgt innerhalb von **30 Tagen** nach Aufforderung.

(4) Die Löschung erfolgt innerhalb von **90 Tagen** nach Vertragsende bzw. nach erfolgter Rückgabe, einschließlich der Löschung bei Unterauftragsverarbeitern. Sie wird auf Verlangen in Textform bestätigt.

(5) Datensicherungen werden im Rahmen der regulären Sicherungszyklen überschrieben. Bis zum vollständigen Überschreiben bleiben sie einer Wiederherstellung entzogen und werden ausschließlich zur Wiederherstellung im Störungsfall vorgehalten. Die maximale Vorhaltedauer entspricht der Löschfrist nach Absatz 4; spätestens **90 Tage** nach Vertragsende sind auch Datensicherungen gelöscht oder überschrieben.

(6) Gesetzliche Aufbewahrungspflichten bleiben unberührt. Betroffene Daten werden für die Dauer der Aufbewahrung in der Verarbeitung eingeschränkt.

§ 10 Haftung

(1) Für die Haftung im Außenverhältnis gilt Art. 82 DSGVO.

(2) Im Innenverhältnis gelten die Haftungsregelungen des Hauptvertrags. Eine Beschränkung der Haftung für Vorsatz und grobe Fahrlässigkeit sowie für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit ist ausgeschlossen.

(3) Im Verhältnis der Parteien zueinander haftet jede Partei entsprechend ihrem Anteil an der Verantwortung für einen Schaden nach Maßgabe des Art. 82 Abs. 2 DSGVO.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen in datenschutzrechtlichen Fragen die Regelungen dieser Vereinbarung vor.

(3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig, Regensburg.

(5) Bestandteil dieser Vereinbarung sind: Anlage 1 (Unterauftragsverarbeiter) und Anlage 2 (Technische und organisatorische Maßnahmen).

Für den Auftraggeber	**Für den Auftragnehmer**
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift
_____	_____
Name, Funktion	Name, Funktion

Anlage 1 — Unterauftragsverarbeiter

Stand: 12.10.2026

#	Unternehmen	Sitz	Leistung / verarbeitete Daten	Ort der Verarbeitung	Drittland
1	**SAS SPOKE** (Dienst „Meeting BaaS") SIREN 883 755 654	35 rue Pauline Borghèse, 92200 Neuilly-sur-Seine, Frankreich	Beitritt des Aufzeichnungsdienstes zu Online-Besprechungen, Aufzeichnung, **Umwandlung Audio→Text (Abschrift)**. *Daten: Audio, Abschrift, Termin- und Teilnehmerdaten*	Scaleway, Paris, Frankreich (EU)	nein
2	**Microsoft Ireland Operations Ltd.** (Dienste „Azure OpenAI" und „Azure AI Speech")	One Microsoft Place, Dublin, Irland	Umwandlung vom Auftraggeber hochgeladener Audioaufnahmen in Text (Abschrift); inhaltliche Auswertung der Abschriften, Einbettungen für die semantische Suche, dialogbasierter Assistent, Kontaktimport mittels großer Sprachmodelle. *Daten: hochgeladene Audioaufnahmen, Abschriften, Protokollinhalte, Fragen des Nutzers, Kontaktdaten*	Europäische Union (EU-Datenzone von Microsoft Azure); Ressourcenstandort Azure OpenAI Frankfurt am Main, Deutschland	nein
3	**Hetzner Online GmbH**	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Betrieb der Server- und Datenbankinfrastruktur (Rechenzentrum Nürnberg). *Daten: sämtliche gespeicherten Daten*	Deutschland	nein
4	**Brevo** (vormals Sendinblue)	Paris, Frankreich	Versand von Transaktions- und Protokoll-E-Mails. *Daten: Empfängeradresse, Name, Protokollinhalt im Anhang*	Europäische Union	nein

Nicht als Unterauftragsverarbeitung erfasst

Microsoft (Graph API) und **Google** (Calendar API) werden ausschließlich angesprochen, um Kalenderdaten aus dem **vom Auftraggeber selbst betriebenen Mandanten** zu lesen. Der Auftraggeber ist gegenüber diesen Anbietern selbst Verantwortlicher; ein eigenes Auftragsverhältnis des Auftragnehmers besteht insoweit nicht.

PDF-Erzeugung. Die Umwandlung der Protokolle in das PDF-Format erfolgt durch einen vom Auftragnehmer selbst betriebenen Dienst auf der eigenen, unter Nr. 3 aufgeführten Infrastruktur (Hetzner Online GmbH). Inhaltsdaten verlassen dabei die Infrastruktur des Auftragnehmers nicht; ein Unterauftragsverhältnis mit einem Dritten besteht insoweit nicht.

Entwicklungs- und Testumgebung. Für Entwicklung und Test betreibt der Auftragnehmer eine von der Produktivumgebung vollständig getrennte Umgebung bei Supabase, Inc. (Region Frankfurt, Deutschland). Dort werden ausschließlich synthetische Testdaten und keine personenbezogenen Daten des Auftraggebers verarbeitet; der Auftragnehmer stellt dies organisatorisch sicher.

Zahlungsabwicklung. Zahlungen werden über die Stripe Payments Europe, Ltd. (Dublin, Irland) abgewickelt. Stripe verarbeitet Zahlungsdaten insoweit als eigenständiger Verantwortlicher; der Auftragnehmer erhält und speichert keine vollständigen Zahlungsdaten (vgl. § 2 Abs. 2).

Weitergabe durch SAS SPOKE

SAS SPOKE setzt nach der Subprozessorenliste seines Data Processing Agreement folgende Unterauftragsverarbeiter ein: **Scaleway** (Hosting und Speicherung; Rechenzentrum Paris, Frankreich; Audio-, Video- und Abschriftsdaten werden dort bei der Übertragung und im Ruhezustand verschlüsselt) sowie **Gladia** (Umwandlung der Aufnahmen in Text; Verarbeitung in Frankreich). Eine Übermittlung in Drittländer findet in dieser Kette nicht statt. Die Aufbewahrungsdauer für Aufzeichnungen und Abschriften ist bei SPOKE nach eigener Angabe auf **maximal 90 Tage** begrenzt.

Sprachverarbeitung durch Microsoft Azure

Die Verarbeitung nach Nr. 2 erfolgt über die Dienste **Azure OpenAI** und **Azure AI Speech** innerhalb der Europäischen Union; die Azure-OpenAI-Ressource des Auftragnehmers ist in Frankfurt am Main (Deutschland) angelegt. Aufnahmen aus Online-Besprechungen werden durch den unter Nr. 1 genannten Unterauftragsverarbeiter in Text umgewandelt; vom Auftraggeber hochgeladene Audioaufnahmen wandelt Azure AI Speech in Text um. Übermittelte Inhalte werden von Microsoft **nicht zum Training oder zur Verbesserung von Modellen** verwendet. Zur Erkennung von Missbrauch speichert Microsoft an Azure OpenAI übermittelte Inhalte für **bis zu 30 Tage** und löscht sie anschließend, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

Das Auftragsverarbeitungsverhältnis mit SAS SPOKE besteht auf Grundlage des von SPOKE gestellten Data Processing Agreement einschließlich Standardvertragsklauseln, das kraft Einbeziehung Bestandteil des Nutzungsvertrags ist (abrufbar unter meetingbaas.com/en/legal/data-processing-agreement). Eine gesonderte Unterzeichnung ist dort nicht vorgesehen.

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

Stand: 12.10.2026. Die Angaben unter 1–4 sind durch eine Sicherheitsprüfung vom 29.07.2026 und durch Auswertung des Quelltextes belegt.

1. Vertraulichkeit

Zutrittskontrolle. Der Betrieb erfolgt in Rechenzentren der Hetzner Online GmbH in Nürnberg. Zutrittsschutz, Videoüberwachung und Zutrittsprotokollierung obliegen dem Betreiber; die Nachweise ergeben sich aus dessen Zertifizierungen.

Zugangskontrolle. Zugriff auf die Verwaltungsebene nur für benannte Personen über persönliche, nicht geteilte Konten. Anwendungsseitige Anmeldung über Kennung und Kennwort; Kennwörter werden ausschließlich als Hash gespeichert.

Zugriffskontrolle. Mandantentrennung auf Datenbankebene über zeilenbasierte Zugriffsregeln (Row Level Security). Jeder Datensatz ist einem Arbeitsbereich zugeordnet; Abfragen werden serverseitig auf die Arbeitsbereiche des anfragenden Nutzers eingeschränkt. Bei leerem Berechtigungsumfang schließt die Prüfung in die sichere Richtung (kein Zugriff statt Vollzugriff). Rollenmodell mit Eigentümer-, Administrator- und Mitgliedsrechten.

Trennungskontrolle. Produktiv- und Entwicklungsumgebung sind vollständig getrennte Systeme mit getrennten Datenbeständen und getrennten Zugangsdaten.

2. Integrität

Übertragungskontrolle. Sämtliche Verbindungen ausschließlich über TLS. Interne Aufrufe zwischen Anwendungskomponenten erfolgen serverseitig.

Verschlüsselung im Ruhezustand. Zugangsschlüssel zu verbundenen Kalendersystemen (Erneuerungstoken) werden vor der Speicherung mit **AES-256 im Galois-Counter-Modus** verschlüsselt. Je Datensatz wird ein neuer zufälliger Initialisierungswert erzeugt. Der Schlüssel wird als Umgebungsvariable außerhalb der Datenbank vorgehalten und ist als nicht auslesbar gekennzeichnet. Ein Versionskennzeichen ermöglicht den Schlüsselwechsel.

Besonderer Schutz der Zugangsschlüssel. Die Tabelle mit den verschlüsselten Erneuerungstoken trägt zeilenbasierten Zugriffsschutz **ohne jede Freigaberegel** — dies bewirkt eine vollständige Sperre für alle Anwendungsrollen. Zusätzlich wurden die Tabellenrechte für die Rollen der Oberfläche entzogen. Es bestehen damit zwei voneinander unabhängige Schranken. Zugriff besteht ausschließlich für die Dienstrolle.

Kurzlebige Zugriffsschlüssel (Gültigkeit 3.600 Sekunden) werden an keiner Stelle gespeichert. Sie bestehen ausschließlich im Arbeitsspeicher der aufrufenden Funktion. Es existiert im Quelltext kein Schreibvorgang in Datenbank, Datei, Zwischenspeicher oder Protokoll, der diese Schlüssel enthält.

Eingabekontrolle. Protokollinhalte sind revisionsfähig angelegt: Änderungen werden als neue Einträge geführt, die Historie bleibt nachvollziehbar. Verarbeitungszeitpunkte werden protokolliert.

3. Verfügbarkeit und Belastbarkeit

Regelmäßige Datensicherung durch den Infrastrukturbetreiber. Überwachung der Kalendersynchronisation mit Alarmierung des Betriebsteams, wenn länger als 30 Minuten kein Abgleich stattgefunden hat. Aktualisierung von Abhängigkeiten nach Sicherheitsmeldungen.

4. Datenminimierung beim Kalenderzugriff

Es werden ausschließlich drei delegierte, **ausnahmslos lesende** Berechtigungen angefordert: Calendars.Read, offline_access, User.Read. Es besteht kein Schreibzugriff auf den Kalender des Auftraggebers und kein Zugriff auf Postfach, Kontakte oder Dateien.

5. Auftragskontrolle

Verpflichtung aller Beschäftigten auf Vertraulichkeit. Weisungsgebundene Verarbeitung. Unterauftragsverarbeiter werden vertraglich auf ein entsprechendes Schutzniveau verpflichtet.

6. Verfahren zur regelmäßigen Überprüfung

Die Anwendung wird regelmäßig sicherheitsgeprüft, zuletzt im Juli 2026 durch eine quelltextbasierte Sicherheitsprüfung nach dem Vorgehen des BSI für Penetrationstests und den Prüfkategorien der OWASP-Leitfäden. Jede Feststellung durchläuft eine gegenläufige Prüfung mit dem Ziel der Widerlegung; festgestellte Punkte werden nach Kritikalität priorisiert und behoben. Auskunft nach § 8 Abs. 5 der Vereinbarung bleibt unberührt.

7. Transparenz gegenüber Betroffenen

Der Aufzeichnungsdienst erscheint bei Online-Besprechungen **sichtbar in der Teilnehmerliste**. Eine verdeckte Aufzeichnung ist nicht vorgesehen. Der Auftraggeber kann eigene Datenschutzhinweise hinterlegen, die automatisch an Termin-Teilnehmer versandt werden.