MITFRAUSCHMIDT

# Vertrag zur Auftragsverarbeitung

gemäß Artikel 28 Datenschutz-Grundverordnung (DSGVO)

**Version 1.0 | Stand: 25. Juli 2026**

Für den Software-Dienst „MitFrauSchmidt“ einschließlich Telefon-, Chat-, E-Mail-, Kalender-, Reporting- und optionaler E-Commerce-Integrationen.

**STATUS: VERTRAGSENTWURF ZUR TECHNISCHEN UND ANWALTLICHEN ENDFREIGABE**

Die Vertragsstruktur ist auf Art. 28 DSGVO und den beschriebenen Produktbetrieb zugeschnitten. Sie darf erst produktiv als zugesicherter Vertragsstandard eingesetzt werden, wenn die Freigabepunkte im Anhang A – insbesondere Azure-Voice-Live-Deployment, Telnyx-Audioverarbeitung, tatsächliche Unterauftragnehmer, Löschautomation und TOM-Umsetzung – technisch bestätigt und dokumentiert sind.

**Elektronischer Abschluss**

Diese Vereinbarung kann in Textform oder elektronisch, insbesondere im Bestell- oder Onboardingprozess, geschlossen werden. Die verwendete Fassung, der Annahmezeitpunkt und die Identität des Kunden sind revisionssicher zu protokollieren.

**Auftragsverarbeiter**

Dennis Beichert · better than e-commerce D. Beichert · Akazienplatz 14 · 65597 Hünfelden · Deutschland

E-Mail: hallo@mit-frau-schmidt.de · Telefon: 06438 9016836 · USt-IdNr.: DE445320469

# Dokumentenstatus und Vertragsparteien

| Feld | Angabe |
|---|---|
| Dokument | Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO |
| Version | 1.0 |
| Rechts- und Redaktionsstand | 25.07.2026 |
| Geltungsbereich | MitFrauSchmidt B2B-SaaS und aktivierte Module |
| Vertragssprache | Deutsch |
| Vorrang | Dieser AVV geht bei Datenschutzfragen widersprechenden Regelungen des Hauptvertrags vor. |

## 1. Verantwortlicher („Kunde“)

| Angabe | Eintrag |
|---|---|
| Firma / Name | _____ |
| Rechtsform | _____ |
| Anschrift | _____ |
| Vertretungsberechtigte Person | _____ |
| Datenschutzkontakt | _____ |
| Kunden-/Vertragsnummer | _____ |

## 2. Auftragsverarbeiter („MitFrauSchmidt“)

| Angabe | Eintrag |
|---|---|
| Anbieter | Dennis Beichert, handelnd unter better than e-commerce D. Beichert |
| Produkt / Marke | MitFrauSchmidt |
| Anschrift | Akazienplatz 14, 65597 Hünfelden, Deutschland |
| Vertretung | Dennis Beichert, Inhaber |
| Datenschutz- und Vertragskontakt | hallo@mit-frau-schmidt.de |
| Telefon | 06438 9016836 |

**Rollenabgrenzung**

Der Kunde ist Verantwortlicher für die im Rahmen seines Betriebs verarbeiteten Anrufer-, Kontakt-, Termin-, E-Mail-, Chat-, Beschäftigten- und Endkundendaten. MitFrauSchmidt verarbeitet diese Daten grundsätzlich als Auftragsverarbeiter. Für eigene Website-, Vertriebs-, Vertrags-, Abrechnungs-, Betrugspräventions- und gesetzliche Nachweisdaten handelt MitFrauSchmidt dagegen als eigener Verantwortlicher; diese Verarbeitung fällt nicht unter diesen AVV.

# Inhaltsübersicht

# Vertrag zur Auftragsverarbeitung

## § 1 Gegenstand, Anwendungsbereich und Rangfolge

**1.1** Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch MitFrauSchmidt im Auftrag des Kunden im Zusammenhang mit dem Hauptvertrag über den Software-Dienst „MitFrauSchmidt“ und den vom Kunden aktivierten Modulen.

**1.2** Der AVV gilt nur, soweit MitFrauSchmidt personenbezogene Daten für Zwecke und nach Weisungen des Kunden verarbeitet. Verarbeitungsvorgänge, bei denen MitFrauSchmidt die Zwecke und wesentlichen Mittel selbst bestimmt, insbesondere eigener Vertrieb, Vertragsverwaltung, Abrechnung, Forderungsmanagement, Missbrauchs- und Betrugsprävention sowie Erfüllung gesetzlicher Pflichten, fallen nicht unter diesen AVV und werden in den eigenen Datenschutzinformationen von MitFrauSchmidt beschrieben.

**1.3** Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV für Fragen des Schutzes personenbezogener Daten vor. Zwingende gesetzliche Vorschriften, insbesondere die DSGVO und anwendbare nationale Datenschutzgesetze, bleiben unberührt.

**1.4** Die Anlagen 1 bis 7 sind Bestandteil dieses AVV. Die Anhänge A bis D dienen der technischen und rechtlichen Freigabe beziehungsweise Dokumentation; sie werden nur dann Vertragsbestandteil, wenn dies ausdrücklich vereinbart ist.

## § 2 Dauer, Art und Zweck der Verarbeitung

**2.1** Die Verarbeitung beginnt erst nach wirksamem Abschluss dieses AVV und technischer Freischaltung der jeweiligen Module. Sie dauert grundsätzlich für die Laufzeit des Hauptvertrags und endet nach vollständiger Rückgabe oder Löschung der Auftragsdaten nach § 16 und Anlage 5.

**2.2** Art, Zweck, Kategorien personenbezogener Daten, Kategorien betroffener Personen, Verarbeitungsschritte und aktivierbare Module sind in Anlage 1 beschrieben. Die tatsächliche Verarbeitung richtet sich nach dem gebuchten Leistungsumfang und den dokumentierten Weisungen des Kunden.

**2.3** MitFrauSchmidt verarbeitet Auftragsdaten ausschließlich zur Bereitstellung, Sicherung, Wartung und vertragsgemäßen Unterstützung des Dienstes. Eine Verarbeitung für eigene Produktwerbung, ein Training allgemeiner KI-Modelle, ein kundenübergreifendes Profiling oder eine sonstige Zweckänderung ist ausgeschlossen, soweit nicht eine eigenständige Rechtsgrundlage, wirksame Anonymisierung oder eine separate Vereinbarung mit dem Kunden besteht.

## § 3 Weisungen und Verantwortlichkeit

**3.1** Der Kunde bleibt für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Rechte betroffener Personen, die Informationspflichten, die Wahl der Rechtsgrundlagen, die Erforderlichkeit der Daten, die Richtigkeit seiner Konfiguration und die Zulässigkeit seiner Weisungen verantwortlich.

**3.2** Mit Abschluss dieses AVV erteilt der Kunde die allgemeine Weisung, Auftragsdaten im Umfang des Hauptvertrags, der Anlagen und seiner im Dashboard oder in Textform vorgenommenen Konfigurationen zu verarbeiten. Einzelweisungen können über dokumentierte Administrationsfunktionen oder in Textform an den Datenschutzkontakt erteilt werden.

**3.3** Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. MitFrauSchmidt dokumentiert wesentliche Weisungen und Änderungen in geeigneter Weise.

**3.4** Hält MitFrauSchmidt eine Weisung für datenschutzrechtswidrig, informiert MitFrauSchmidt den Kunden unverzüglich. Die Ausführung darf bis zur Bestätigung oder Änderung der Weisung ausgesetzt werden, soweit dies zum Schutz betroffener Personen erforderlich ist.

**3.5** Ist MitFrauSchmidt durch Unionsrecht oder das Recht eines Mitgliedstaats zu einer Verarbeitung außerhalb der Kundenweisung verpflichtet, informiert MitFrauSchmidt den Kunden vor der Verarbeitung über diese Pflicht, sofern das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

## § 4 Pflichten des Auftragsverarbeiters

**4.1** MitFrauSchmidt verarbeitet Auftragsdaten nur auf dokumentierte Weisung des Kunden und stellt sicher, dass die Anforderungen aus Art. 28 Abs. 3 DSGVO eingehalten werden.

**4.2** MitFrauSchmidt unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Erfüllung seiner Pflichten aus Art. 12 bis 22, 32 bis 36 DSGVO sowie bei aufsichtsbehördlichen Anfragen, soweit diese die Auftragsverarbeitung betreffen.

**4.3** MitFrauSchmidt führt ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO, soweit gesetzlich erforderlich, und stellt auf Anfrage die zur Rechenschaftslegung notwendigen Informationen bereit.

**4.4** MitFrauSchmidt berichtigt, löscht, sperrt, exportiert oder schränkt Auftragsdaten nur auf Weisung des Kunden ein, soweit nicht eine gesetzliche Pflicht entgegensteht.

**4.5** MitFrauSchmidt informiert den Kunden, wenn eine betroffene Person, Behörde oder ein sonstiger Dritter unmittelbar Ansprüche oder Auskunftsersuchen in Bezug auf Auftragsdaten an MitFrauSchmidt richtet. Eine inhaltliche Beantwortung erfolgt grundsätzlich nur nach Weisung des Kunden, sofern keine gesetzliche Pflicht zur unmittelbaren Antwort besteht.

## § 5 Vertraulichkeit und eingesetzte Personen

**5.1** MitFrauSchmidt setzt nur Personen ein, die auf Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind und die Auftragsdaten nur im erforderlichen Umfang verarbeiten dürfen.

**5.2** Berechtigungen werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben, regelmäßig überprüft und nach Aufgabenwechsel oder Ausscheiden unverzüglich angepasst beziehungsweise entzogen.

**5.3** Support- oder Administrationszugriffe auf Kundeninhalte erfolgen nur, wenn sie zur Störungsbehebung, zur Umsetzung einer Kundenweisung, zur Sicherheit oder zur Erfüllung gesetzlicher Pflichten erforderlich sind. Solche Zugriffe werden, soweit technisch möglich und verhältnismäßig, protokolliert.

## § 6 Technische und organisatorische Maßnahmen

**6.1** MitFrauSchmidt trifft und unterhält die in Anlage 3 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Die Maßnahmen gewährleisten unter Berücksichtigung von Stand der Technik, Implementierungskosten, Art, Umfang, Umständen und Zwecken der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken ein dem Risiko angemessenes Schutzniveau.

**6.2** Die Maßnahmen dürfen im technischen Fortschritt weiterentwickelt oder durch mindestens gleichwertige Maßnahmen ersetzt werden, sofern das vereinbarte Sicherheitsniveau nicht unterschritten wird und wesentliche Änderungen dokumentiert werden.

**6.3** Der Kunde ist für die Sicherheit seiner Endgeräte, Benutzerkonten, Rufumleitungen, Zugangsdaten, OAuth-Freigaben, angebundenen Systeme sowie für die angemessene Vergabe eigener Rollen und Rechte verantwortlich.

**6.4** Die TOM-Anlage ist vor produktiver Verwendung technisch zu bestätigen. Nicht implementierte oder nicht verifizierte Zusicherungen dürfen nicht gegenüber Kunden als bestehender Standard dargestellt werden.

## § 7 Besondere Datenkategorien und sensible Einsatzfälle

**7.1** Im normalen Betrieb können Anrufer oder Kommunikationspartner freiwillig oder situationsbedingt besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, strafrechtlich relevante Angaben, Notfallinformationen oder Daten schutzbedürftiger Personen mitteilen. MitFrauSchmidt fordert solche Daten nicht pauschal an und verarbeitet sie nur, soweit dies durch die Konfiguration und Weisung des Kunden gedeckt und für den jeweiligen Vorgang erforderlich ist.

**7.2** Der Kunde prüft vor Aktivierung von Notfall-Triage, Gesundheits-, Pflege-, Personal-, Rechts-, Finanz- oder vergleichbar sensiblen Anwendungsfällen die Rechtsgrundlage, Erforderlichkeit, Informationspflichten und gegebenenfalls die Pflicht zur Datenschutz-Folgenabschätzung.

**7.3** MitFrauSchmidt erteilt keine medizinische, rechtliche oder sicherheitsfachliche Beratung. Notfallfunktionen dürfen ausschließlich vom Kunden freigegebene, eng begrenzte Hinweise und Eskalationsregeln verwenden und ersetzen weder den Notruf noch eine fachliche Gefahrenbeurteilung.

**7.4** Eine Nutzung für automatisierte Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung, insbesondere Beschäftigtenauswahl, Kreditwürdigkeit, Versicherung, medizinische Diagnostik oder Leistungsentscheidungen, ist ohne gesonderte schriftliche Vereinbarung, Risikoprüfung und erforderliche Schutzmaßnahmen unzulässig.

## § 8 Betroffenenrechte

**8.1** MitFrauSchmidt unterstützt den Kunden durch geeignete technische und organisatorische Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und gegebenenfalls der Überprüfung automatisierter Entscheidungen.

**8.2** Der Kunde nutzt vorrangig bereitgestellte Export-, Such-, Berichtigungs- und Löschfunktionen. Soweit zusätzliche Unterstützung erforderlich ist, konkretisiert er das Ersuchen, die betroffene Person, den Zeitraum und die verlangte Maßnahme.

**8.3** MitFrauSchmidt antwortet auf ein hinreichend bestimmtes Unterstützungsersuchen unverzüglich und grundsätzlich innerhalb von fünf Arbeitstagen mit einer Eingangsbestätigung und einem Umsetzungsstatus. Gesetzliche Fristen des Kunden bleiben unberührt.

## § 9 Datenschutzverletzungen und Sicherheitsereignisse

**9.1** MitFrauSchmidt informiert den Kunden über eine Verletzung des Schutzes personenbezogener Auftragsdaten unverzüglich nach Bekanntwerden, grundsätzlich innerhalb von 24 Stunden, soweit zu diesem Zeitpunkt hinreichende Tatsachen vorliegen. Eine schrittweise Nachmeldung bleibt zulässig.

**9.2** Die Meldung enthält, soweit verfügbar, Art des Vorfalls, betroffene Systeme und Datenkategorien, ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen, getroffene oder geplante Abhilfemaßnahmen, Ansprechpartner sowie bekannte Drittanbieterbezüge.

**9.3** MitFrauSchmidt trifft unverzüglich angemessene Maßnahmen zur Eingrenzung, Beweissicherung, Wiederherstellung und Vermeidung weiterer Schäden und unterstützt den Kunden bei der Bewertung von Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

**9.4** Die Entscheidung über Meldungen an Aufsichtsbehörden oder betroffene Personen obliegt grundsätzlich dem Kunden. MitFrauSchmidt darf eigene gesetzliche Meldepflichten erfüllen und stimmt sich, soweit zulässig, mit dem Kunden ab.

## § 10 Datenschutz-Folgenabschätzung und Behördenkonsultation

**10.1** MitFrauSchmidt stellt dem Kunden die zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlichen, bei MitFrauSchmidt verfügbaren Informationen über Verarbeitung, Systeme, Risiken, Unterauftragnehmer, Datenflüsse, Löschfristen und Sicherheitsmaßnahmen bereit.

**10.2** Soweit eine vorherige Konsultation nach Art. 36 DSGVO erforderlich ist, unterstützt MitFrauSchmidt den Kunden im angemessenen Umfang. Die Verantwortung für Durchführung, Ergebnis, Freigabe und Dokumentation der Datenschutz-Folgenabschätzung verbleibt beim Kunden, soweit nicht MitFrauSchmidt für eigene Verarbeitungsvorgänge selbst verantwortlich ist.

## § 11 Unterauftragnehmer

**11.1** Der Kunde erteilt MitFrauSchmidt eine allgemeine schriftliche Genehmigung zum Einsatz der in Anlage 4 aufgeführten Unterauftragnehmer für die dort beschriebenen Leistungen.

**11.2** MitFrauSchmidt informiert den Kunden mindestens 30 Kalendertage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragnehmers in Textform oder über ein dokumentiertes Kundenportal. Bei dringenden sicherheits- oder verfügbarkeitsbedingten Änderungen kann die Frist verkürzt werden; die Gründe sind mitzuteilen.

**11.3** Der Kunde kann einer Änderung innerhalb von 14 Kalendertagen nach Zugang aus objektiv nachvollziehbaren Datenschutzgründen widersprechen. Die Parteien bemühen sich um eine zumutbare Lösung. Ist keine Lösung

möglich, kann jede Partei das betroffene Modul außerordentlich beenden; der übrige Vertrag bleibt bestehen, soweit zumutbar.

**11.4** MitFrauSchmidt schließt mit Unterauftragnehmern Verträge, die mindestens gleichwertige Datenschutzpflichten enthalten, insbesondere zu Weisungsbindung, Vertraulichkeit, Sicherheit, Unterstützung, Löschung, Audits und Drittlandtransfers. MitFrauSchmidt bleibt gegenüber dem Kunden für die Pflichterfüllung der Unterauftragnehmer verantwortlich.

**11.5** Nicht jeder vom Kunden direkt gewählte oder vertraglich gebundene Plattformanbieter ist Unterauftragnehmer von MitFrauSchmidt. Die Abgrenzung von Kundensystemen und Unterauftragnehmern richtet sich nach § 13 und Anlage 4.

## § 12 Drittlandübermittlungen

**12.1** Eine Übermittlung oder ein Zugriff auf Auftragsdaten außerhalb des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind und die Übermittlung von der Weisung und Leistungsbeschreibung gedeckt ist.

**12.2** Soweit kein Angemessenheitsbeschluss nach Art. 45 DSGVO greift, verwendet MitFrauSchmidt geeignete Garantien, insbesondere die jeweils anwendbaren EU-Standardvertragsklauseln, bei Unterauftragnehmerketten regelmäßig Modul 3 (Auftragsverarbeiter an Unterauftragsverarbeiter), ergänzt um erforderliche Transfer-Risikobewertungen und zusätzliche Schutzmaßnahmen.

**12.3** Wird das EU-US Data Privacy Framework als Übermittlungsgrundlage genutzt, prüft MitFrauSchmidt, ob die Zertifizierung des konkreten US-Empfängers gültig ist und die betroffene Datenart sowie Dienstleistung umfasst. Bei Wegfall wird auf eine andere zulässige Grundlage umgestellt oder die Verarbeitung ausgesetzt.

**12.4** Globale oder nicht geografisch begrenzte KI- und Cloud-Deployments dürfen für Auftragsdaten nur nach vorheriger transparenter Information, dokumentierter Weisung und datenschutzrechtlicher Prüfung eingesetzt werden. EU-geografische beziehungsweise regionale Deployments sind zu bevorzugen.

## § 13 Kundeneigene Konten, OAuth und Fremdsysteme

**13.1** Der Kunde kann eigene Konten und Systeme, insbesondere Google Workspace/Gmail, Microsoft 365/Graph, Kalender, WhatsApp Business, Shopify, WooCommerce oder vergleichbare Dienste, über OAuth, API-Schlüssel oder andere Schnittstellen anbinden.

**13.2** Soweit der Kunde mit dem Plattformanbieter selbst in Vertragsbeziehung steht und MitFrauSchmidt lediglich auf Weisung des Kunden über dessen Konto zugreift, gilt der Plattformanbieter grundsätzlich als Kundensystem und nicht als Unterauftragnehmer von MitFrauSchmidt. Der Kunde bleibt für Auswahl, Vertrag, Rechtsgrundlage, Konfiguration, Aufbewahrung und Drittlandtransfers dieses Systems verantwortlich.

**13.3** Soweit MitFrauSchmidt ein eigenes Plattformkonto, einen eigenen Mandanten oder einen eigenen Vertrag mit dem Plattformanbieter nutzt, um Auftragsdaten zu verarbeiten, ist der Anbieter als Unterauftragnehmer zu behandeln und vor Einsatz in Anlage 4 aufzunehmen.

**13.4** MitFrauSchmidt beschränkt OAuth-Berechtigungen auf erforderliche Scopes, speichert Tokens verschlüsselt beziehungsweise in einem geeigneten Secrets-System, protokolliert wesentliche Verbindungsereignisse und ermöglicht den Widerruf der Verbindung. Der Kunde kann die Berechtigung jederzeit im angebundenen System entziehen.

**13.5** Daten, die nach Übertragung im Kundensystem gespeichert werden, unterliegen den Lösch- und Aufbewahrungsregeln des Kunden und des jeweiligen Plattformanbieters. MitFrauSchmidt löscht eigene Zwischenspeicher nach Anlage 5.

## § 14 KI-spezifische Verarbeitung und EU AI Act

**14.1** MitFrauSchmidt verwendet KI-Modelle ausschließlich zur Erbringung der vom Kunden beauftragten Funktionen. Auftragsdaten, Prompts, Transkripte, E-Mail-Inhalte und Ausgaben dürfen nicht zum Training oder zur Verbesserung allgemein verfügbarer Modelle von MitFrauSchmidt oder Unterauftragnehmern verwendet werden, soweit nicht eine getrennte, freiwillige und widerrufliche Vereinbarung oder eine wirksame Anonymisierung vorliegt.

**14.2** MitFrauSchmidt dokumentiert die für produktive Module freigegebenen Modellanbieter, Dienste, Deployment-Arten und geografischen Verarbeitungsgrenzen gemäß Anlage 6. Nicht freigegebene globale Deployments und Consumer-Konten sind unzulässig.

**14.3** Der Dienst ist so zu konfigurieren, dass Personen zu Beginn einer sprachlichen oder textlichen Interaktion verständlich darüber informiert werden, dass sie mit einem KI-System interagieren, sofern dies nicht offensichtlich ist. Der Kunde darf den vorgesehenen KI-Hinweis nicht deaktivieren oder verschleiern.

**14.4** MitFrauSchmidt unterstützt menschliche Kontrolle, insbesondere durch Freigabeprozesse, Eskalationen, Kennzeichnung von Unsicherheit und die Möglichkeit, Vorgänge an Menschen zu übergeben. Der Kunde entscheidet, welche Ausgaben ohne weitere Prüfung verwendet werden dürfen.

**14.5** Der Kunde stellt keine verbotenen oder nicht freigegebenen Einsatzwecke ein und informiert MitFrauSchmidt über branchenspezifische regulatorische Anforderungen. Die datenschutzrechtlichen Rollen aus diesem AVV bestimmen nicht abschließend die Rollen als Anbieter, Betreiber/Deployer, Bevollmächtigter oder sonstiger Akteur nach dem EU AI Act.

**14.6** Modell- oder Providerwechsel, die zu einem neuen Unterauftragnehmer, einer Drittlandübermittlung, einer wesentlichen Zweckänderung oder einem erheblich veränderten Risiko führen, unterliegen den Informations- und Widerspruchsregeln dieses AVV.

## § 15 Nachweise, Audits und Kontrollen

**15.1** MitFrauSchmidt stellt dem Kunden auf Anfrage alle erforderlichen Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO bereit, insbesondere diesen AVV, TOM-Dokumentation, Unterauftragnehmerliste, Löschkonzept, relevante Zertifikate, Auditberichte oder vergleichbare Nachweise, soweit verfügbar und ohne Rechte Dritter zu verletzen.

**15.2** Der Kunde kann höchstens einmal jährlich und zusätzlich bei konkretem Anlass eine Prüfung durchführen oder durch einen zur Verschwiegenheit verpflichteten unabhängigen Prüfer durchführen lassen. Dokumentenprüfungen und anerkannte Prüfberichte haben Vorrang vor Vor-Ort-Prüfungen.

**15.3** Vor-Ort-Prüfungen sind mindestens 20 Arbeitstage vorher anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf den erforderlichen Umfang zu begrenzen. Sicherheit, Vertraulichkeit und Rechte anderer Kunden dürfen nicht beeinträchtigt werden. Rechte von Aufsichtsbehörden bleiben unberührt.

**15.4** MitFrauSchmidt darf schutzwürdige Informationen, insbesondere Sicherheitsdetails, Geschäftsgeheimnisse und Daten anderer Kunden, angemessen schwärzen oder durch gleichwertige Nachweise ersetzen, sofern der Prüfzweck erreichbar bleibt.

## § 16 Rückgabe, Löschung und Vertragsende

**16.1** Nach Ende der Auftragsverarbeitung löscht oder gibt MitFrauSchmidt nach Wahl des Kunden sämtliche Auftragsdaten gemäß Anlage 5 zurück, sofern keine unions- oder mitgliedstaatliche Aufbewahrungspflicht entgegensteht.

**16.2** Der Kunde kann während des Vertrags und innerhalb des in Anlage 5 genannten Exportfensters verfügbare Daten exportieren. Nach Ablauf der Fristen werden Produktivdaten und anschließend Sicherungskopien nach dem dokumentierten Rotationsverfahren gelöscht beziehungsweise unbrauchbar überschrieben.

**16.3** Gesetzlich aufzubewahrende Daten werden von operativen Systemen getrennt, in der Verarbeitung beschränkt und nach Ablauf der Pflicht gelöscht. MitFrauSchmidt informiert den Kunden über die betreffende Pflicht, soweit rechtlich zulässig.

**16.4** Die Löschung umfasst keine Daten, für die MitFrauSchmidt als eigener Verantwortlicher eine eigenständige gesetzliche Aufbewahrungspflicht oder Rechtsgrundlage hat; diese Daten werden zweckgebunden und getrennt verarbeitet.

## § 17 Mitwirkung und Kosten

**17.1** Die im gewöhnlichen Umfang erforderliche Unterstützung bei Betroffenenrechten, Datenschutzverletzungen, Nachweisen und Standardauskünften ist mit der vereinbarten Vergütung abgegolten.

**17.2** Außergewöhnliche, wiederholte oder durch rechtswidrige beziehungsweise fehlerhafte Kundenweisungen verursachte Zusatzaufwände können nach vorheriger Information zu den vereinbarten oder marktüblichen Sätzen berechnet werden, soweit dies nicht die gesetzlich geschuldete Unterstützung aushöhlt.

## § 18 Haftung und zwingendes Recht

**18.1** Die Haftung der Parteien richtet sich nach Art. 82 DSGVO, den sonstigen zwingenden gesetzlichen Vorschriften und den wirksamen Haftungsregelungen des Hauptvertrags. Rechte betroffener Personen und Befugnisse der Aufsichtsbehörden werden durch diesen AVV nicht beschränkt.

**18.2** Jede Partei informiert die andere unverzüglich über geltend gemachte Ansprüche oder behördliche Maßnahmen, soweit sie die Auftragsverarbeitung betreffen, und unterstützt eine abgestimmte Sachverhaltsaufklärung.

## § 19 Laufzeit und Beendigung

**19.1** Dieser AVV tritt mit elektronischer Annahme, Unterzeichnung oder dem im Hauptvertrag bestimmten Zeitpunkt in Kraft, jedoch spätestens vor Beginn der Auftragsverarbeitung.

**19.2** Er endet mit vollständiger Beendigung der Auftragsverarbeitung und Erfüllung der Rückgabe- und Löschpflichten. Datenschutz-, Vertraulichkeits-, Nachweis- und Löschpflichten wirken fort, soweit ihr Zweck dies erfordert.

**19.3** Ein isoliertes ordentliches Kündigungsrecht des AVV besteht nicht, solange der Hauptvertrag eine Auftragsverarbeitung erfordert. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

## § 20 Änderungen und elektronische Kommunikation

**20.1** Änderungen dieses AVV bedürfen mindestens der Textform oder eines dokumentierten elektronischen Änderungsverfahrens. Dies gilt nicht für zulässige Weiterentwicklungen gleichwertiger TOM, Aktualisierungen von Kontaktdaten oder Änderungen der Unterauftragnehmer nach dem vereinbarten Verfahren.

**20.2** Mitteilungen nach diesem AVV können an die in Anlage 2 benannten Kontakte oder über das Kundenportal erfolgen. Der Kunde hält seine Kontakte aktuell und stellt sicher, dass Mitteilungen zu Datenschutz und Sicherheit intern bearbeitet werden.

## § 21 Schlussbestimmungen

**21.1** Es gilt deutsches Recht, soweit dem keine zwingenden datenschutzrechtlichen Kollisionsnormen entgegenstehen.

**21.2** Gerichtsstand richtet sich nach dem Hauptvertrag und zwingendem Recht. Zuständigkeiten von Datenschutzaufsichtsbehörden und Rechte betroffener Personen bleiben unberührt.

**21.3** Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Regelung durch eine wirksame Regelung, die dem datenschutzrechtlichen Schutzzweck am nächsten kommt.

# Anlage 1 – Beschreibung der Verarbeitung

> **Modularer Umfang**
> Es werden nur die Module und Datenkategorien verarbeitet, die der Kunde tatsächlich aktiviert und konfiguriert. Nicht aktivierte optionale Module sind nicht Gegenstand der laufenden Verarbeitung.

## 1. Gegenstand und Zwecke

- Annahme und Bearbeitung eingehender Telefonanrufe im Namen des Kunden einschließlich Live-Sprachverarbeitung, Anliegenaufnahme, Klassifizierung, Terminwunsch, Rückruf- und Eskalationslogik.
- Bereitstellung eines KI-Chat-Assistenten auf Websites oder anderen digitalen Kontaktpunkten des Kunden.
- Analyse und Unterstützung bei E-Mail-Kommunikation, insbesondere Sortierung, Priorisierung und Erstellung von Antwortentwürfen.
- Lesen und Schreiben freigegebener Kalenderdaten sowie Terminbuchung nach Kundenregeln.
- Erstellung von Tages- und Vorgangsberichten, optionaler Versand über E-Mail oder WhatsApp Business.
- Verarbeitung von Firmenwissen, FAQs, Leistungsdaten, Öffnungszeiten, Preis- oder Prozessinformationen zur Beantwortung von Kundenanliegen.
- Optional: Nachschlagen von Bestellungen, Kundenkonten, Versand- oder Retourenstatus in angebundenen E-Commerce-Systemen.
- Betrieb, Mandantentrennung, Fehleranalyse, Sicherheit, Support, Abrechnung von Nutzungsvolumen und technische Protokollierung.

## 2. Verarbeitungstätigkeiten und Module

| Modul | Typische Verarbeitung | Aktivierung |
|---|---|---|
| Telefon | Empfang von Verbindungsdaten und Live-Audiostream; Speech-to-Text; KI-Antwort; Text-to-Speech; Speicherung von Transkript und Vorgang; Weiterleitung/Eskalation. | Nur bei Buchung und Rufumleitung |
| Chat | Empfang von Chattext, Kontext, technischen Metadaten und optional Kontaktdaten; Erzeugung von Antworten und Leads. | Nur bei eingebautem/aktiviertem Widget |
| E-Mail | OAuth-/API-Zugriff; Lesen, Klassifizieren, Extrahieren; Erstellen von Entwürfen; optionaler Versand nur nach freigegebener Regel. | Nur nach OAuth-Freigabe |
| Kalender | Verfügbarkeitsabfrage, Terminlesen/-schreiben, Kontakt- und Notizdaten. | Nur nach OAuth-Freigabe |
| Reporting | Verdichtung von Vorgängen; Zustellung per Dashboard, E-Mail oder optional WhatsApp. | Nach Kundenkonfiguration |
| Wissensbasis | Upload/Import von Betriebswissen und Dokumenten; Indexierung/Retrieval; Nutzung als Antwortkontext. | Nach Upload/Einrichtung |
| E-Commerce | Abruf von Bestell-, Liefer-, Retouren- und Kundendaten; Ausgabe im Gespräch/Chat. | Optional, gesonderte Anbindung |
| Support/Sicherheit | Logs, Zugriffsereignisse, Fehlermeldungen, Incident-Analyse, Backups und Wiederherstellung. | Notwendiger Plattformbetrieb |

## 3. Kategorien personenbezogener Daten

- Stammdaten: Name, Firma, Funktion, Kundennummer, Anrede, interne Zuordnungen.

- Kontaktdaten: Telefonnummern, E-Mail-Adressen, Anschriften, Messenger-Kennungen.
- Kommunikations- und Inhaltsdaten: Gesprächsinhalte, Transkripte, Chatverläufe, E-Mail-Inhalte, Anhänge, Notizen, Antwortentwürfe.
- Termin- und Kalenderdaten: Datum, Uhrzeit, Ort, Anlass, Teilnehmende, Verfügbarkeiten und Kalendernotizen.
- Vorgangs-, Angebots-, Auftrags- und Servicedaten: Anliegen, Priorität, Kategorie, Status, Rückruf, Reklamation, Angebot, Leistung, Notfallkennzeichen.
- E-Commerce-Daten: Bestellnummer, Bestellpositionen, Lieferstatus, Retourenstatus, Kundenzuordnung und Zahlungsstatus, jedoch grundsätzlich keine vollständigen Zahlungskartendaten.
- Technische und Nutzungsdaten: IP-Adresse, Geräte-/Browserdaten, Zeitstempel, Session-/Mandantenkennung, API- und OAuth-Ereignisse, Fehler- und Sicherheitslogs.
- Berechtigungs- und Konfigurationsdaten: Benutzerrollen, Freigaben, Eskalationskontakte, Regeln, Wissensquellen und OAuth-Tokens.
- Potenziell besondere Kategorien nach Art. 9 DSGVO oder sensible Inhalte, wenn sie von Anrufern, Absendern oder Nutzern mitgeteilt werden, etwa Gesundheits-, Unfall-, Pflege-, Religions- oder Gewerkschaftsbezug. Diese Daten sind nicht Standardzweck und unterliegen § 7.

## 4. Kategorien betroffener Personen

- Kunden, Interessenten, Anrufer, Website- und Chat-Nutzer des Kunden.
- E-Mail-Absender und -Empfänger, Termininteressenten und Terminteilnehmer.
- Endkunden, Besteller, Empfänger, Retouren- und Servicekunden im E-Commerce.
- Beschäftigte, freie Mitarbeitende, Bewerber, Lieferanten, Partner und Ansprechpartner des Kunden.
- Notfallkontakte, Bereitschaftsdienste und sonstige vom Kunden benannte Empfänger.
- Benutzer und Administratoren des MitFrauSchmidt-Kundenkontos.

## 5. Frequenz und Umfang

Die Verarbeitung erfolgt fortlaufend beziehungsweise anlassbezogen während der Nutzung. Umfang und Zahl der betroffenen Personen hängen vom Kommunikationsaufkommen des Kunden, der Zahl angebundener Konten, den aktivierten Modulen und den konfigurierten Aufbewahrungsfristen ab.

# Anlage 2 – Weisungen und Ansprechpartner

## 1. Standardweisungen

| Bereich | Dokumentierte Weisung |
|---|---|
| Verarbeitung | Bereitstellung der aktivierten Module ausschließlich für Zwecke des Kunden. |
| Speicherung | Speicherung in den freigegebenen Regionen und innerhalb der festgelegten Löschfristen. |
| KI | Nutzung nur freigegebener Enterprise-/API-Dienste; keine Verwendung für allgemeines Modelltraining. |
| Telefon | Keine aktivierte Gesprächsaufzeichnung durch MitFrauSchmidt; Live-Verarbeitung und Speicherung des Texttranskripts/Vorgangs nach Kundenkonfiguration. |
| E-Mail | Antworten grundsätzlich als Entwurf; automatischer Versand nur nach ausdrücklich aktivierter, dokumentierter Regel. |
| Kalender | Lesen/Schreiben nur in freigegebenen Kalendern und Scopes. |
| Notfall | Nur kundenseitig freigegebene Hinweise und Eskalationsketten; kein Ersatz für Notruf oder Fachberatung. |
| Drittanbieter | Einsatz nur nach Anlage 4 und § 11/12. |
| Löschung | Fristen nach Anlage 5, soweit nicht der Kunde kürzere Fristen konfiguriert. |

## 2. Ansprechpartner Kunde

| Funktion | Name | E-Mail / Telefon |
|---|---|---|
| Vertragsverantwortung | _____ | _____ |
| Datenschutz | _____ | _____ |
| IT/Sicherheit | _____ | _____ |
| Notfall/Eskalation | _____ | _____ |

## 3. Ansprechpartner MitFrauSchmidt

| Funktion | Kontakt |
|---|---|
| Vertrag / Datenschutz | Dennis Beichert · hallo@mit-frau-schmidt.de · 06438 9016836 |
| Sicherheitsvorfälle | hallo@mit-frau-schmidt.de; Betreff „DATENSCHUTZVORFALL – DRINGEND“ |
| Support / Weisungen | hallo@mit-frau-schmidt.de |

**Empfohlene organisatorische Verbesserung**

Vor breitem Produktivbetrieb sollten eigene Funktionsadressen wie datenschutz@mit-frau-schmidt.de und security@mit-frau-schmidt.de eingerichtet, überwacht und in Incident-Runbooks hinterlegt werden. Bis dahin bleibt die veröffentlichte Adresse hallo@mit-frau-schmidt.de maßgeblich.

# Anlage 3 – Technische und organisatorische Maßnahmen (TOM)

**Verbindlichkeit erst nach technischer Bestätigung**

Die folgenden Maßnahmen bilden den zugesicherten Mindeststandard für den Produktivbetrieb. Vor Verwendung dieser Fassung ist jede Maßnahme anhand der realen Infrastruktur zu bestätigen. Abweichungen sind zu dokumentieren und müssen ein mindestens gleichwertiges Schutzniveau gewährleisten.

## 1. Governance, Datenschutzorganisation und Risikomanagement

- Dokumentierte Verantwortlichkeiten für Datenschutz, Informationssicherheit, Incident Response, Provider-Management und Freigaben.
- Regelmäßige Risikobewertung der Plattform, insbesondere Telefonie, KI-Modelle, OAuth-Integrationen, Mandantentrennung, Notfalllogik und Drittlandzugriffe.
- Verzeichnis der Verarbeitungstätigkeiten und aktueller Datenflussplan.
- Dokumentierte Auswahl- und Kontrollprozesse für Unterauftragnehmer einschließlich DPA, Transfergrundlage, Sicherheitsnachweise und Änderungsmonitoring.
- Vertraulichkeitsverpflichtungen und regelmäßige Datenschutz-/Sicherheitssensibilisierung für zugriffsberechtigte Personen.

## 2. Zutrittskontrolle

- Produktivserver in professionell gesicherten Rechenzentren; physischer Zutritt liegt beim Rechenzentrumsanbieter und ist vertraglich sowie organisatorisch kontrolliert.
- Keine lokale Speicherung produktiver Kundendaten auf ungeschützten privaten Geräten oder frei zugänglichen Datenträgern.
- Arbeitsgeräte mit Bildschirmsperre, Geräteschutz und angemessener physischer Aufbewahrung.

## 3. Zugangs- und Authentisierungskontrolle

- Individuelle Benutzerkonten; keine gemeinsam genutzten administrativen Identitäten, soweit technisch vermeidbar.
- Mehrfaktor-Authentisierung für privilegierte Zugänge, Hosting-, Cloud-, Datenbank-, Provider- und Quellcodekonten.
- Starke Passwortregeln, sichere Wiederherstellungsverfahren und Sperrung beziehungsweise Rate Limiting gegen automatisierte Angriffe.
- Zugriff auf Admin- und interne Systeme nur über verschlüsselte Verbindungen; zusätzliche Netz- oder IP-Beschränkungen, soweit angemessen.

## 4. Berechtigungs- und Zugriffskontrolle

- Rollen- und mandantenbezogene Berechtigungen nach Least Privilege.
- Serverseitige Autorisierungsprüfung für jede kundenbezogene Aktion; öffentliche Bot- oder Widget-IDs gewähren keinen administrativen Zugriff.
- Regelmäßige Überprüfung privilegierter Rechte sowie unverzüglicher Entzug bei Rollenwechsel oder Ausscheiden.
- Supportzugriffe auf Inhalte nur anlassbezogen, dokumentiert und auf das erforderliche Minimum beschränkt.

## 5. Mandantentrennung und Zweckbindung

- Logische Trennung aller Kundendaten durch unveränderliche Mandantenkennungen und serverseitige Zugriffskontrollen.
- Automatisierte Tests gegen Cross-Tenant-Zugriffe und IDOR-Schwachstellen vor Releases und bei wesentlichen Änderungen.
- Keine Verwendung produktiver Kundendaten in Entwicklungs- oder Testumgebungen, außer nach dokumentierter Freigabe und angemessener Pseudonymisierung.

- Getrennte Speicherbereiche beziehungsweise Schlüssel/Namespaces, soweit technisch und wirtschaftlich angemessen.

## 6. Übertragungs- und Transportkontrolle

- TLS-verschlüsselte Übertragung für Web, API, Datenbankzugriffe, Providerkommunikation und administrative Zugänge; veraltete Protokolle werden deaktiviert.
- Signierte und authentisierte Webhooks; Schutz vor Replay-Angriffen, soweit vom jeweiligen Anbieter unterstützt.
- Keine Übertragung vertraulicher Inhalte über unverschlüsselte Standardkanäle.
- Drittland- und Regionseinstellungen werden dokumentiert und gegen die Freigabeliste geprüft.

## 7. Speicher-, Verschlüsselungs- und Geheimnisschutz

- Verschlüsselung von Datenträgern, Datenbanken oder Backups im Ruhezustand durch provider- oder anwendungsseitige Mechanismen nach Stand der Technik.
- API-Schlüssel, OAuth-Tokens, Passwörter und sonstige Secrets werden nicht im Quellcode oder Klartext-Logs gespeichert, sondern in einem geeigneten Secret-Management-System geschützt.
- Schlüssel- und Secret-Rotation bei Verdacht, Personalwechsel oder planmäßiger Überprüfung.
- Besonders sensible Felder werden, soweit möglich, zusätzlich minimiert, maskiert oder verschlüsselt.

## 8. Eingabe-, Änderungs- und Protokollkontrolle

- Protokollierung sicherheitsrelevanter Anmelde-, Admin-, Berechtigungs-, OAuth-, Lösch-, Export- und Konfigurationsereignisse.
- Schutz der Logs vor unbemerkter Veränderung und Zugriff nur für berechtigte Personen.
- Keine unnötige Protokollierung vollständiger Gesprächs-, E-Mail- oder Token-Inhalte; Maskierung sensibler Werte.
- Zeitquellen und Zeitstempel werden konsistent gehalten, um Ereignisse nachvollziehen zu können.

## 9. Verfügbarkeitskontrolle, Backup und Wiederherstellung

- Regelmäßige, automatisierte und verschlüsselte Sicherungen der erforderlichen Produktivdaten mit dokumentierter Rotation.
- Getrennte Aufbewahrung von Sicherungen und eingeschränkte Wiederherstellungsberechtigungen.
- Regelmäßige, dokumentierte Wiederherstellungstests und Behebung festgestellter Mängel.
- Monitoring zentraler Dienste, Ressourcen, Fehlerraten, Providerverbindungen und Backup-Jobs mit Alarmierung.

## 10. Integrität, sichere Entwicklung und Schwachstellenmanagement

- Versionskontrolle, Review wesentlicher Codeänderungen und getrennte Freigabe-/Deploymentprozesse.
- Regelmäßige Aktualisierung von Betriebssystemen, Bibliotheken, Containern und Abhängigkeiten nach risikobasierter Priorität.
- Automatisierte Abhängigkeits- und Geheimnisscans sowie Behandlung kritischer Sicherheitsmeldungen.
- Eingabevalidierung, Schutz vor Injection, CSRF, XSS, SSRF, Prompt Injection und missbräuchlicher Werkzeugnutzung entsprechend dem jeweiligen Modul.
- Sicherheitsprüfung vor wesentlichen Releases und nach erheblichen Architekturänderungen.

## 11. KI- und Sprachsicherheit

- Freigabeliste für Modelle, Endpoints, Regionen und Deploymenttypen; Consumer-Zugänge und nicht geprüfte globale Deployments sind ausgeschlossen.
- Systemprompts, Werkzeugrechte und Wissensquellen werden mandantenbezogen getrennt und gegen Prompt-Injection-Risiken abgesichert.
- Ausgaben mit höherem Risiko werden durch Freigabe, Eskalation oder klare Leistungsgrenzen abgesichert.
- Keine dauerhafte Audioaufzeichnung durch die Anwendung; flüchtige Streaming-Puffer werden nach Beendigung der Echtzeitverarbeitung verworfen. Providerseitige Sicherheitsverarbeitungen sind separat vertraglich zu prüfen.

- Konfiguration, Modellversion und wesentliche Antwortpfade werden für Fehleranalyse und Nachvollziehbarkeit angemessen dokumentiert, ohne mehr Inhaltsdaten als erforderlich zu speichern.

## 12. Löschung und Datenminimierung

- Technisch umgesetzte Löschjobs nach Anlage 5 mit Erfolgs-/Fehlerprotokollierung.
- Kundenkonfigurierbare kürzere Fristen, soweit der Dienst dies unterstützt.
- Unverzügliche Deaktivierung und Löschung widerrufener OAuth-Tokens und nicht mehr erforderlicher Integrationsdaten.
- Datenexport und anschließende sichere Löschung bei Vertragsende; definierter Nachlauf für Backups.

## 13. Incident Response und Kontinuität

- Dokumentierter Prozess für Erkennung, Klassifizierung, Eindämmung, Beweissicherung, Kommunikation und Nachbereitung von Sicherheitsvorfällen.
- Erreichbarer Meldeweg und Eskalationskette; unverzügliche Kundeninformation nach § 9.
- Dokumentation von Ursachen, Auswirkungen, Maßnahmen und Lessons Learned.
- Wiederkehrende Überprüfung und Übung des Incident-Prozesses.

## 14. Regelmäßige Wirksamkeitskontrolle

- Mindestens jährliche Überprüfung der TOM und zusätzlich bei wesentlichen Änderungen oder Vorfällen.
- Regelmäßige Prüfung von Benutzerrechten, Unterauftragnehmern, Drittlandmechanismen, Löschjobs, Backups, Logs und KI-Deployments.
- Dokumentierte Nachverfolgung von Feststellungen mit Verantwortlichem und Frist.

# Anlage 4 – Unterauftragnehmer, optionale Dienste und Kundensysteme

**Wichtig zur Liste**

Die nachfolgende Liste ist auf Basis des beschriebenen Systems erstellt. Vor Unterzeichnung sind aktive Vertragspartner, Kontoinhaber, Produktnamen, Regionen und DPA-Versionen mit den echten Accounts abzugleichen. Ein Anbieter ist nur dann freigegeben, wenn sein Status und die besonderen Bedingungen erfüllt sind.

## A. Freigegebene beziehungsweise freizugebende Unterauftragnehmer

| | |
|---|---|
| **Anbieter / Vertragspartner** | Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland |
| **Status / Rolle** | Unterauftragnehmer – Hosting/Infrastruktur; produktiv nur mit abgeschlossenem Hetzner-AVV |
| **Leistung** | Server, Datenbank, Speicher, Backups und Netzwerkbetrieb |
| **Datenkategorien** | Sämtliche in Anlage 1 genannten Auftragsdaten, soweit im Plattformbetrieb gespeichert |
| **Ort / Drittlandmechanismus** | Deutschland beziehungsweise gewählte EU-Rechenzentrumsregion \| Kein Drittlandtransfer bei EU-Konfiguration; Unterauftragnehmerliste des Anbieters beachten |
| **Besondere Bedingungen** | Konkrete Serverstandorte und Backupregionen dokumentieren; keine unbeabsichtigte Replikation außerhalb der freigegebenen Region. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | sipgate GmbH, Gladbacher Straße 74, 40219 Düsseldorf, Deutschland |
| **Status / Rolle** | Unterauftragnehmer – Telefonie, soweit Vertrag/Konto von MitFrauSchmidt geführt wird |
| **Leistung** | Rufnummern, SIP/Weiterleitung, Verbindungsaufbau und Telekommunikationsmetadaten |
| **Datenkategorien** | Rufnummern, Verbindungs- und Routingdaten, gegebenenfalls Audioübertragung |
| **Ort / Drittlandmechanismus** | Deutschland/EU nach konkretem Tarif und AVV \| Drittlandzugriffe anhand Anbieterunterlagen prüfen |
| **Besondere Bedingungen** | sipgate-AVV abschließen; Tarif, Subprozessoren, Verkehrs-/Abrechnungsdaten und Aufbewahrung dokumentieren. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | Microsoft Ireland Operations Limited / Microsoft Azure |
| **Status / Rolle** | Unterauftragnehmer – Speech-to-Text, Text-to-Speech und gegebenenfalls Voice Live |
| **Leistung** | Echtzeit-Spracherkennung, Sprachausgabe, Gesprächs-KI/Modellinferenz |
| **Datenkategorien** | Live-Audiostream, Antworttext, Transkript-/Promptausschnitte, technische Metadaten |
| **Ort / Drittlandmechanismus** | Azure Speech: germanywestcentral; Voice Live nur freigegebenes EU-Data-Zone- oder regionales Deployment \| Microsoft DPA; bei Drittlandzugriffen geeignete Mechanismen einschließlich SCC/Angemessenheitsgrundlage |
| **Besondere Bedingungen** | GLOBAL STANDARD ist ohne gesonderte Prüfung und Weisung unzulässig. Endpoint, Modell, Deploymenttyp, Logging/Retention und Content-Safety-Datenflüsse vor Go-live nachweisen. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | united-domains AG, Gautinger Straße 10, 82319 Starnberg, Deutschland |
| **Status / Rolle** | Unterauftragnehmer – System-E-Mail, soweit Postfach/Konto von MitFrauSchmidt geführt wird |
| **Leistung** | Versand und Empfang von Systembenachrichtigungen, Leads, Support- und Berichts-E-Mails |
| **Datenkategorien** | E-Mail-Adressen, Header-/Metadaten, Nachrichteninhalte und Anhänge |
| **Ort / Drittlandmechanismus** | Deutschland nach Anbieterangaben für E-Mail-Hosting \| Kein Drittlandtransfer vorgesehen; Subprozessoren prüfen |
| **Besondere Bedingungen** | Online-AVV abschließen und Postfach-Aufbewahrung, Spam-/Malwarefilter sowie Backups dokumentieren. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | Amazon Web Services EMEA SARL / Amazon Bedrock |
| **Status / Rolle** | Optionaler/geplanter Unterauftragnehmer – KI-Inferenz nach produktiver Migration |
| **Leistung** | Verarbeitung von Prompts, Gesprächs-/E-Mail-Ausschnitten und Antwortgenerierung über Bedrock |
| **Datenkategorien** | Textinhalte, Kontext, technische Inferenzmetadaten; keine Audioverarbeitung, sofern nicht gesondert aktiviert |
| **Ort / Drittlandmechanismus** | Quellregion eu-central-1; ausschließlich EU-geografisches Cross-Region-Inference-Profil oder regionales Deployment \| AWS DPA; EU-geografische Verarbeitung; SCC für etwaige zulässige Drittlandzugriffe |
| **Besondere Bedingungen** | Globale Inference-Profile deaktivieren. Retention auf „nicht speichern“ beziehungsweise minimal konfigurieren. Modellanbieter ist bei Bedrock nur dann zusätzlich als Unterauftragnehmer zu listen, wenn er tatsächlich Zugriff auf Kundendaten erhält. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | Anthropic PBC, USA |
| **Status / Rolle** | Bedingter Unterauftragnehmer – nur solange eine direkte Anthropic-API produktiv verwendet wird |
| **Leistung** | KI-Inferenz für Chat, Entwürfe oder andere Textfunktionen |
| **Datenkategorien** | Prompts, Gesprächs-/E-Mail-Ausschnitte, Ausgaben und technische Metadaten |
| **Ort / Drittlandmechanismus** | USA \| Gültige EU-US-DPF-Zertifizierung oder SCC Modul 3 plus Transferprüfung |
| **Besondere Bedingungen** | Nach vollständiger Migration auf AWS Bedrock ohne Anthropic-Datenzugriff aus der aktiven Liste entfernen. Direkte Consumer-/Webkonten sind für Auftragsdaten unzulässig. Zero-Retention/No-Training-Vertragseinstellungen bestätigen. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | Telnyx LLC, USA |
| **Status / Rolle** | BEDINGT / FREIGABEGESPERRT – Telefonieunterauftragnehmer, falls technisch erforderlich |
| **Leistung** | Carrier-, Rufnummern-, SIP-, Media-Streaming- und Routingdienste |
| **Datenkategorien** | Rufnummern, Verbindungsdaten, Netzwerk- und Audio-Stream; gegebenenfalls Sicherheits-/Fraud-Samples |
| **Ort / Drittlandmechanismus** | USA und globale Telekommunikationsinfrastruktur \| Nur bei gültiger DPF-Abdeckung oder SCC Modul 3, Transferprüfung und zusätzlichen Maßnahmen |
| **Besondere Bedingungen** | Vor Produktivbetrieb schriftlich klären: DPA/Vertragspartner, Subprozessoren, Routing, Supportzugriffe, Aufbewahrung und insbesondere automatische Audio-Sampling-/Analysefunktionen. Bis zur Klärung keine Aussage „nirgendwo Audioaufzeichnung“ und möglichst technische/vertragliche Deaktivierung oder Migration auf EU-Anbieter. |

| | |
|---|---|
| **Anbieter / Vertragspartner** | WhatsApp Ireland Limited / Meta Platforms Ireland Limited (je nach konkretem Produktvertrag) |
| **Status / Rolle** | Optionaler Unterauftragnehmer oder Kundensystem – Einordnung nach Kontoinhaber und Vertrag |
| **Leistung** | Versand von Tagesberichten und Benachrichtigungen über WhatsApp Business Platform |
| **Datenkategorien** | Telefonnummer, Nachrichten-/Berichtsinhalt, Zustell- und Nutzungsmetadaten |
| **Ort / Drittlandmechanismus** | EU und mögliche Drittlandweitergaben innerhalb der Meta-/WhatsApp-Gruppe \| Business Data Processing Terms, Data Transfer Addendum, DPF/SCC nach konkretem Setup |
| **Besondere Bedingungen** | Nur opt-in aktivieren; sensible Inhalte minimieren; Inhalt des Tagesreports konfigurierbar machen; Konto-/Vertragsinhaber und Rollen vor Go-live eindeutig dokumentieren. |

## B. Kundensysteme – grundsätzlich keine Unterauftragnehmer von MitFrauSchmidt

| System | Typische Einordnung | Verantwortung / Bedingung |
|---|---|---|
| Google Workspace / Gmail / Google Calendar | Kundensystem, wenn der Kunde selbst Vertrag und Konto hält. | Kunde prüft Vertrag, Rechtsgrundlage, Regionen und Drittlandtransfers. MitFrauSchmidt beschränkt OAuth-Scopes und löscht eigene Tokens/Cache. |
| Microsoft 365 / Outlook / Graph / Kalender | Kundensystem, wenn der Kunde selbst Vertrag und Tenant hält. | Wie vor; Azure-Sprachdienste im MitFrauSchmidt-Konto bleiben dagegen Unterauftragnehmer. |
| Shopify / WooCommerce / Shop-Hosting | Kundensystem bei kundeneigenem Shopvertrag. | Nur erforderliche Bestell- und Servicedaten abrufen; keine Zahlungskartendaten; Rechte und Löschregeln des Shops beachten. |
| Kundeneigenes WhatsApp-Business-Konto | Kundensystem, wenn Vertrag/Konto direkt beim Kunden liegt und MitFrauSchmidt nur autorisiert zugreift. | Rollen anhand Cloud-API-/BSP-Setup prüfen; bei MitFrauSchmidt-eigenem Konto wird Meta/WhatsApp Unterauftragnehmer. |
| Kundeneigene Telefonanlage / Festnetzanbieter | Kundensystem für die Ausgangsrufnummer und Rufumleitung. | Kunde ist für Zulässigkeit, Beschäftigteninformation und Rufumleitung verantwortlich; MitFrauSchmidt für eigene Zielnummern-/Carrierkette. |

## C. Eigene Verantwortlichkeit außerhalb dieses AVV

| Anbieter / Vorgang | Einordnung |
|---|---|
| Stripe Payments Europe, Limited / Zahlungsabwicklung | Je nach Funktion eigener Verantwortlicher und/oder Auftragsverarbeiter von MitFrauSchmidt für Vertrags- und Zahlungsdaten. Zahlungsdaten des MitFrauSchmidt-Kunden fallen grundsätzlich nicht unter die Auftragsverarbeitung für dessen Anrufer/Endkunden und werden in den eigenen Datenschutzinformationen geregelt. |
| Steuerberatung, Banken, Behörden, Rechtsberatung | Empfänger oder eigene Verantwortliche im Rahmen gesetzlicher Pflichten und Unternehmensverwaltung; nicht Teil der kundenbezogenen Auftragsverarbeitung. |
| Eigene Website-Analytics und Werbung | Eigene Verantwortlichkeit von MitFrauSchmidt; Einwilligungs- und Transparenzpflichten werden in der Website-Datenschutzerklärung geregelt. |

# Anlage 5 – Lösch- und Rückgabekonzept

**Vertraglicher Standard**

Die folgenden Fristen sind belastbare Standardwerte für einen SaaS-Betrieb, müssen jedoch technisch umgesetzt und fachlich bestätigt werden. Der Kunde kann kürzere Fristen konfigurieren, soweit keine gesetzlichen oder zwingenden technischen Gründe entgegenstehen. Eine Verlängerung bedarf einer dokumentierten Kundenweisung oder Rechtsgrundlage.

| Datenart | Standardfrist / Ereignis | Löschregel |
|---|---|---|
| Live-Audiostream und flüchtige Audiopuffer | Nur für die Dauer der Echtzeitverarbeitung | MitFrauSchmidt aktiviert keine dauerhafte Gesprächsaufzeichnung; flüchtige Puffer werden nach Ende des Streams verworfen. Carrierseitige Sicherheitsverarbeitung bleibt nach Anlage 4 gesondert zu klären. |
| Transkript eines Telefonats | 90 Tage nach Gesprächsende oder Vorgangsabschluss | Automatische Löschung; kundenkonfigurierbar grundsätzlich zwischen 7 und 365 Tagen. Kürzere Frist geht vor. |
| Strukturierter Vorgang / Lead / Rückruf | 180 Tage nach Abschluss oder letzter Bearbeitung | Löschung oder Anonymisierung; offene Vorgänge werden nicht allein wegen Zeitablauf gelöscht, solange der Kunde sie aktiv bearbeitet. |
| Chatverlauf | 90 Tage nach letzter Interaktion | Automatische Löschung; Kontakt-/Lead-Datensatz kann nach eigener Frist fortbestehen. |
| E-Mail-Inhalte und Entwürfe im MitFrauSchmidt-Speicher | 90 Tage nach Abschluss/Freigabe; Cache 7 Tage | Originale im Kundenpostfach unterliegen dessen Regeln. Tokens und Cache werden bei Trennung der Integration gelöscht. |
| Kalendercache und Verfügbarkeitsdaten | Maximal 7 Tage | Kalendereinträge im Kundensystem bleiben nach Kundenregeln erhalten; eigener Cache wird gelöscht. |
| Tagesberichte im Dashboard | 30 Tage nach Erstellung | Nachrichten beim Empfänger/WhatsApp unterliegen dem Kundensystem und Plattformanbieter. |
| Wissensbasis und Kundendokumente | Während Vertragslaufzeit; 30 Tage nach Modul-/Vertragsende | Exportmöglichkeit; anschließend Produktivlöschung, sofern keine kürzere Weisung. |
| OAuth-Tokens / API-Zugangsdaten | Bis Widerruf oder Trennung der Integration | Unverzügliche Deaktivierung und Löschung; technische Sicherungskopien nach Backuprotation. |
| Raw Server-/Anwendungslogs | 30 Tage | Automatische Rotation; Inhalte werden minimiert und sensible Werte maskiert. |
| Sicherheits- und Admin-Auditlogs | 180 Tage | Danach Löschung oder Aggregation, sofern kein Incident/Legal Hold besteht. |
| Supportfälle mit Kundeninhalten | 180 Tage nach Abschluss | Frühere Löschung auf Weisung, soweit Supportnachweis nicht mehr erforderlich. |
| Backups | Rollierend 35 Tage | Gelöschte Produktivdaten verschwinden spätestens mit Ablauf der Rotation; Zielwert maximal 45 Tage. Backups werden nicht für operative Zwecke reaktiviert, außer zur Wiederherstellung. |
| Vertragsende – Exportfenster | 14 Tage ab Vertragsende | Kunde kann verfügbare Daten exportieren; auf Wunsch kann unmittelbar gelöscht werden. |
| Vertragsende – Produktivdaten | Spätestens 30 Tage nach Ende des Exportfensters | Vollständige Löschung oder Rückgabe nach Kundenwahl; Bestätigung auf Anfrage. |
| Vertragsende – verbleibende Backups | Spätestens 60 Tage nach Produktivlöschung | Nur technisch bedingter Nachlauf; Zugriff gesperrt und Löschung durch Rotation. |

## 1. Legal Hold und gesetzliche Aufbewahrung

Eine Aussetzung der Löschung („Legal Hold“) erfolgt nur bei dokumentierter gesetzlicher Pflicht, vollstreckbarer behördlicher/gerichtlicher Anordnung oder ausdrücklicher rechtmäßiger Kundenweisung. Betroffene Daten werden gekennzeichnet, in ihrer Verarbeitung beschränkt und nach Wegfall des Grundes gelöscht.

## 2. Löschprotokoll

Automatisierte Löschjobs sollen Erfolg, Fehler, betroffene Datenklasse und Zeitpunkt protokollieren, ohne gelöschte Inhalte erneut zu speichern. Wiederholte Fehler lösen eine technische Eskalation aus.

## 3. Anonymisierung

Anstelle einer Löschung ist eine weitere Nutzung nur zulässig, wenn eine irreversible Anonymisierung erreicht ist und eine Re-Identifizierung mit allen vernünftigerweise verfügbaren Mitteln ausgeschlossen ist. Bloße Pseudonymisierung reicht nicht aus.

# Anlage 6 – KI-, Modell- und Deployment-Regeln

| Kontrollpunkt | Verbindliche Regel |
|---|---|
| Freigegebene Zugänge | Nur Enterprise-/API-/Cloud-Verträge mit DPA, No-Training-Zusage und dokumentierter Datenregion. Keine Eingabe von Auftragsdaten in Consumer-Chats. |
| Azure Speech | Speech-to-Text und Text-to-Speech über die freigegebene Ressource in germanywestcentral; Endpoints und Schlüssel regionstreu. |
| Azure Voice Live | Nur EU Data Zone oder ausdrücklich regionales Deployment. Global Standard/Global Provisioned nur nach gesonderter Transfer- und Risikoprüfung sowie Kundeninformation. |
| AWS Bedrock | Nur EU-geografisches Cross-Region-Inference-Profil oder regionales Deployment; Global Cross-Region Inference ist für Auftragsdaten deaktiviert. |
| Anthropic direkt | Nur bis zur dokumentierten Migration und nur mit DPA, zulässiger Transfergrundlage, No-Training/Retention-Einstellungen und Eintrag in Anlage 4. |
| Training / Verbesserung | Keine Nutzung von Auftragsdaten für allgemeines Training, Fine-Tuning, menschliche Qualitätsprüfung oder Provider-Produktverbesserung, außer separat vereinbart oder wirksam anonymisiert. |
| Inhaltsprotokollierung | Provider-Logging/Retention auf den technisch möglichen Minimalwert setzen; keine dauerhafte Content-Logging-Funktion ohne dokumentierten Zweck und Frist. |
| Modellwechsel | Vor produktiver Umstellung Datenschutz-, Sicherheits-, Region-, Retention-, Unterauftragnehmer- und Qualitätsprüfung; wesentliche Änderungen nach § 11/14 mitteilen. |
| Werkzeuge / Aktionen | Tool-Aufrufe nur mit minimalen Rechten, serverseitiger Autorisierung, Mandantenprüfung, Eingabevalidierung und Freigabe bei risikoreichen Aktionen. |
| Human Oversight | E-Mail-Versand, verbindliche Zusagen, Preis-/Vertragsaussagen, sensible Eskalationen und rechtlich erhebliche Entscheidungen benötigen kundenseitig definierte Kontrolle. |
| Transparenz | Jede nicht offensichtlich KI-basierte Interaktion beginnt mit einem verständlichen KI-Hinweis. Im Telefonkanal wird der Hinweis gesprochen; im Chat sichtbar dargestellt. |
| Notfälle | Nur freigegebene Eskalationsregeln und Sicherheitstexte; bei unklarer oder akuter Gefahr Hinweis auf menschliche Hilfe/Notruf nach Kundenvorgabe; keine Diagnose. |
| Qualität und Halluzinationen | Antworten werden auf freigegebenes Wissen und definierte Grenzen gestützt; Unsicherheit führt zu Rückfrage, Übergabe oder Nichtbeantwortung statt erfundener Angaben. |

## Freigaberegister (vom Betreiber zu pflegen)

| Modul | Provider / Modell | Endpoint / Region | Deploymenttyp | Retention | Freigabe / Datum |
|---|---|---|---|---|---|
| Telefon STT | _____ | _____ | _____ | _____ | _____ |
| Telefon TTS | _____ | _____ | _____ | _____ | _____ |
| Voice Live / LLM | _____ | _____ | _____ | _____ | _____ |
| Chat / Mail LLM | _____ | _____ | _____ | _____ | _____ |
| Embeddings / RAG | _____ | _____ | _____ | _____ | _____ |

# Anlage 7 – Incident- und Unterstützungsprozess

| Priorität | Beispiel | Erste Maßnahme / Kommunikation |
|---|---|---|
| P1 – kritisch | Bestätigter unbefugter Zugriff auf mehrere Mandanten; Cross-Tenant-Leak; kompromittierte Admin-Zugangsdaten; Verlust besonderer Datenkategorien. | Sofortige Eindämmung; Krisenteam; Kundenmeldung grundsätzlich innerhalb 24 Stunden; fortlaufende Updates. |
| P2 – hoch | Begrenzter Datenabfluss eines Mandanten; falsch adressierter Bericht; unbefugter Supportzugriff; kompromittiertes OAuth-Token. | Token/Access sperren; Umfang sichern; Kunde unverzüglich informieren; Risiko bewerten. |
| P3 – mittel | Sicherheitsrelevanter Konfigurationsfehler ohne bestätigten Datenzugriff; fehlgeschlagener Löschjob; überlange Log-Aufbewahrung. | Beheben, dokumentieren, Risiko prüfen; Kunde informieren, wenn Rechte/Pflichten betroffen sein können. |
| P4 – niedrig | Vermutung oder Fehlalarm ohne Anhaltspunkt für personenbezogene Daten. | Untersuchen und dokumentieren; Eskalation bei neuen Erkenntnissen. |

## Mindestinhalt einer Vorfallmeldung

- Datum/Uhrzeit der Entdeckung und – soweit bekannt – des Beginns und Endes.
- Betroffene Kunden, Module, Systeme, Provider, Regionen und Mandanten.
- Betroffene Datenkategorien, besondere Daten, ungefähre Zahl Personen und Datensätze.
- Bekannte oder wahrscheinliche Ursache, Angriffsweg und Auswirkungen.
- Sofortmaßnahmen, Wiederherstellung, Beweissicherung und geplante Abhilfe.
- Bewertung, ob Daten abgeflossen, verändert, gelöscht oder unzugänglich wurden.
- Kontakt für Rückfragen und Zeitpunkt des nächsten Updates.

## Unterstützung bei Betroffenenanfragen

| Schritt | Vorgehen |
|---|---|
| 1. Eingang | Kunde übermittelt Identifikationsmerkmale, Zeitraum, Module und verlangtes Recht. |
| 2. Suche | MitFrauSchmidt sucht in eigenen produktiven Systemen und veranlasst erforderliche Anfragen bei Unterauftragnehmern. |
| 3. Sicherung | Bei Löschersuchen werden rechtmäßige Aufbewahrungs-/Legal-Hold-Gründe geprüft; ansonsten Löschung/Anonymisierung. |
| 4. Nachweis | Ergebnis, Datenquellen, Ausnahmen und Umsetzungszeitpunkt werden dem Kunden dokumentiert. |
| 5. Antwort | Der Kunde beantwortet die betroffene Person; MitFrauSchmidt antwortet nur bei eigener gesetzlicher Pflicht. |

# Vertragsschluss

Die Parteien bestätigen, dass sie den Inhalt dieses AVV einschließlich der als Vertragsbestandteil bezeichneten Anlagen zur Kenntnis genommen haben. Bei elektronischem Abschluss ersetzt der dokumentierte Annahmevorgang die handschriftliche Unterzeichnung.

| Für den Verantwortlichen | Für den Auftragsverarbeiter |
|---|---|
| Ort, Datum: _____ | Ort, Datum: _____ |
| Name/Funktion: _____ | Dennis Beichert, Inhaber |
| Unterschrift / elektronische Annahme | Unterschrift / elektronische Annahme |

# Anhang A – Freigabesperren vor Produktivbetrieb

**Nicht Vertragsbestandteil – operative Freigabeliste**

Kein skalierter automatisierter Verkauf und keine Verarbeitung echter Kundendaten, bevor alle roten Punkte geklärt sind. Dieser Anhang schützt davor, vertraglich Sicherheits- oder Regionalzusagen zu machen, die technisch noch nicht bewiesen sind.

| Nr. | Prüfpunkt | Done-Kriterium | Status |
|---|---|---|---|
| 1 | Azure Voice Live | Endpoint, Ressource, Modell und Deploymenttyp aus Produktionskonfiguration belegen. Nur EU Data Zone oder ausdrücklich regional. | OFFEN / P0 |
| 2 | Telnyx | DPA, konkrete juristische Einheit, DPF/SCC, Subprozessoren, Routing, Supportzugriffe und Audio-Sampling-Klausel schriftlich klären oder Telnyx aus der Kette entfernen. | OFFEN / P0 |
| 3 | Direkte Anthropic-Nutzung | Produktionscode und Umgebungsvariablen prüfen. Entweder vollständig auf AWS Bedrock EU migrieren oder Anthropic als aktiven US-Unterauftragnehmer vertraglich und technisch absichern. | OFFEN / P0 |
| 4 | Unterauftragnehmerkonten | Für jeden Provider klären, ob MitFrauSchmidt oder der Kunde Kontoinhaber/Vertragspartner ist; daraus Rolle ableiten. | OFFEN / P0 |
| 5 | TOM-Nachweis | MFA, Mandantentrennung, Verschlüsselung at rest, Secret Management, Backups/Restore, Logging, Löschjobs und Supportzugriffe technisch testen und dokumentieren. | OFFEN / P0 |
| 6 | Löschautomation | Fristen aus Anlage 5 in Datenbank, Jobs, Backups, Providerlogs und Kundendashboard implementieren und mit Testdatensätzen nachweisen. | OFFEN / P0 |
| 7 | Produkt-Datenschutzhinweise | Telefon-, Transkript-, Termin-, E-Mail-, Kalender-, WhatsApp-, Provider-, Drittland-, Lösch- und Betroffenenprozesse vollständig in den Produktinformationen ergänzen. | OFFEN / P0 |
| 8 | DSFA | Plattformweite DSFA für Telefon-/KI-/Notfallbetrieb durchführen oder nachvollziehbar dokumentieren, weshalb im konkreten Scope kein hohes Risiko verbleibt. | OFFEN / P0 |
| 9 | Telefonhinweis | Kurzen KI- und Datenschutzhinweis je Kunde bereitstellen; URL/Informationsweg des Verantwortlichen hinterlegen; Tests für alle Gesprächspfade. | OFFEN / P0 |

| Nr. | Prüfpunkt | Done-Kriterium | Status |
|---|---|---|---|
| 10 | Provider-DPAs | Hetzner, sipgate, Microsoft, united-domains, AWS/Anthropic, Telnyx und Meta/WhatsApp je nach Aktivierung abschließen, versionieren und im Nachweisordner ablegen. | OFFEN / P0 |
| 11 | Audio-Claim | Website/Vertrag präzise auf „MitFrauSchmidt speichert im Kundensystem keine Audiodatei“ begrenzen, solange carrierseitige Sicherheitsverarbeitungen nicht ausgeschlossen sind. | OFFEN / P0 |
| 12 | Incident-Prozess | Security-Kontakt, 24/7-Erreichbarkeit für P1, Runbook, Vorlagen und Testübung einrichten. | OFFEN / P1 |

## Empfohlener Nachweisordner

/compliance/01-datenfluss · /02-avv · /03-tom · /04-unterauftragnehmer · /05-loeschkonzept · /06-dsfa · /07-ai-act · /08-incident-response · /09-provider-vertraege · /10-sicherheitstests · /11-claims-nachweise

# Anhang B – DSFA-Schwellenwerttest nach Art. 35 DSGVO

**Vorläufiges Ergebnis**

Für den beschriebenen Plattformbetrieb sprechen mehrere Risikokriterien gleichzeitig für eine vollständige Datenschutz-Folgenabschätzung, insbesondere innovative Sprach-/KI-Technologie, systematische Klassifizierung, Verknüpfung von Telefon/E-Mail/Kalender/Shop, potenziell besondere Daten und Notfallinhalte sowie die geplante Skalierung auf viele Kunden. Ein bloßer Satz „DSFA nicht erforderlich“ wäre ohne belastbare Gegenprüfung nicht vertretbar.

| Kriterium | Bewertung für MitFrauSchmidt | Relevanz |
|---|---|---|
| Neue/innovative Technologie | Echtzeit-Sprach-KI, LLM-Orchestrierung, automatisierte Klassifizierung, OAuth- und Tool-Nutzung. | hoch |
| Systematische Beobachtung/Bewertung | Regelmäßige Erfassung und Klassifizierung von Kommunikationsvorgängen, Priorität und Notfallsignalen. | hoch |
| Besondere/sensible Daten | Gesundheits-, Unfall-, Pflege-, Beschäftigten- oder andere sensible Angaben können spontan auftreten. | mittel bis hoch |
| Datenabgleich/Zusammenführung | Telefon, Chat, E-Mail, Kalender, Wissensbasis und E-Commerce können zusammengeführt werden. | hoch |
| Umfang/Skalierung | Mandantenfähige SaaS-Plattform; Umfang steigt mit Kunden- und Kontaktzahl. | abhängig, bei Skalierung hoch |
| Vulnerable Personen | Notfälle, Pflege-/Gesundheitskontext, Beschäftigte oder sonstige schutzbedürftige Personen möglich. | abhängig vom Kunden |
| Automatisierte Entscheidungen | Standardmäßig unterstützende Klassifizierung; rechtlich erhebliche Entscheidungen sollen ausgeschlossen sein. | mittel |
| Verhinderung von Rechten/Diensten | Fehlklassifizierung kann Erreichbarkeit, Termin oder Notfallweiterleitung beeinflussen. | mittel bis hoch |

## Empfehlung

- Vor dem breiten Produktivbetrieb eine plattformweite DSFA für den Kernprozess Telefon + Voice Live + Transkript + Notfall-/Eskalationslogik durchführen.
- Je Kundenbranche ein Kurzscreening im Onboarding; für Gesundheitswesen, Pflege, Personal, Rechts-/Finanzberatung und umfangreiche besondere Daten gegebenenfalls kundenspezifische DSFA.
- Risiken und Maßnahmen mindestens zu Transparenz, Fehlklassifizierung, Halluzination, Notfall, Drittlandzugriff, Audioverarbeitung, Mandantentrennung, OAuth-Missbrauch, Prompt Injection, Betroffenenrechten und Löschung bewerten.
- Restrisiko und Freigabe durch eine benannte verantwortliche Person dokumentieren; bei verbleibend hohem Risiko vorherige Konsultation nach Art. 36 DSGVO prüfen.

# Anhang C – Erforderliche Ergänzung der Produkt-Datenschutzhinweise

Die öffentlich abrufbare Datenschutzerklärung beschreibt Website, Formulare, Chat und Kunden-Dashboard, muss für den Produktivdienst jedoch zusätzlich mindestens folgende Punkte transparent abdecken:

- Rollenverteilung: Kundenbetrieb als Verantwortlicher für Anrufer-/Endkundendaten; MitFrauSchmidt als Auftragsverarbeiter.
- Telefonieprozess einschließlich Rufumleitung, Carrier, Live-Audiostream, Speech-to-Text, Text-to-Speech, Voice Live, Transkript und strukturierter Vorgang.
- Präzise Aussage zur Audioverarbeitung: keine absichtliche Audiodatei im MitFrauSchmidt-Kundensystem; etwaige carrierseitige Sicherheitsverarbeitungen transparent und vertraglich geklärt.
- Kategorien betroffener Personen und Daten, einschließlich potenziell besonderer Kategorien und Notfallangaben.
- E-Mail-, Kalender-, OAuth-, WhatsApp-, Wissensbasis- und E-Commerce-Integrationen.
- Aktuelle Unterauftragnehmer, Regionen, Drittlandtransfers und Transfermechanismen.
- Konkrete Löschfristen beziehungsweise Kundenkonfiguration nach Anlage 5.
- Betroffenenrechte und praktische Kontaktwege über den jeweiligen Kundenbetrieb.
- KI-Transparenz, Leistungsgrenzen, menschliche Kontrolle und Umgang mit Notfällen.
- Supportzugriffe, Logs, Backups, Sicherheitsmaßnahmen und Incident-Kommunikation in angemessener Transparenz.

## Vorschlag für den kurzen Gesprächsbeginn

> **Telefonhinweis – Vorlage**
>
> „Guten Tag, hier ist die KI-Assistenz von [KUNDENBETRIEB]. Ich nehme Ihr Anliegen im Auftrag des Betriebs auf und wandle das Gespräch live in Text um. Im MitFrauSchmidt-Kundensystem wird keine Audiodatei gespeichert. Weitere Datenschutzhinweise finden Sie unter [DATENSCHUTZ-URL]. Bei akuter Gefahr wählen Sie bitte 112. Wie kann ich Ihnen helfen?“

Der Wortlaut ist je Branche und Gesprächslänge anzupassen. Die kurze Ansage ersetzt nicht die vollständigen Informationen nach Art. 13/14 DSGVO; diese müssen leicht zugänglich bereitgestellt werden. Eine absolute Aussage zur gesamten Carrierkette darf erst nach Klärung von Telnyx und sonstigen Telefonieanbietern verwendet werden.

# Anhang D – Rechts- und Prüfgrundlagen

Berücksichtigt wurden insbesondere folgende Rechtsakte und Leitlinien in der bis 25.07.2026 veröffentlichten Fassung:

- Verordnung (EU) 2016/679 (DSGVO), insbesondere Art. 5, 24, 25, 28, 30, 32 bis 36, 44 bis 49 und 82.
- Durchführungsbeschluss (EU) 2021/915 der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern nach Art. 28 Abs. 7 DSGVO.
- Durchführungsbeschluss (EU) 2021/914 der Kommission über Standardvertragsklauseln für Drittlandübermittlungen.
- EDSA/EDPB Guidelines 07/2020 zu den Begriffen Verantwortlicher und Auftragsverarbeiter, finale Version 2.1.
- EDPB Opinion 22/2024 zu Pflichten bei Auftragsverarbeiter- und Unterauftragsverarbeiterketten.
- Verordnung (EU) 2024/1689 (EU AI Act), insbesondere Transparenzpflichten für interaktive KI-Systeme.
- Verordnung (EU) 2026/1744, veröffentlicht am 24.07.2026, zur Vereinfachung der Umsetzung des EU AI Act; die besondere Übergangsregel bis 02.12.2026 betrifft Art. 50 Abs. 2 für bereits vor dem 02.08.2026 bereitgestellte Systeme zur Erzeugung synthetischer Inhalte und verschiebt nicht den für die Telefon-KI relevanten Interaktionshinweis nach Art. 50 Abs. 1.
- Anwendbares deutsches Datenschutzrecht einschließlich BDSG und TDDDG sowie allgemeine zivil-, wettbewerbs- und strafrechtliche Vorgaben, soweit einschlägig.

## Technische Prüfquellen

- Microsoft-Dokumentation zu Azure Speech-Regionen und Voice-Live-/Deploymenttypen.
- AWS-Dokumentation zu geografischem Cross-Region Inference, Bedrock-Datenschutz, Retention und AWS DPA.
- Offizielle DPA-/Datenschutz-/Subprozessorunterlagen von Hetzner, sipgate, united-domains, Microsoft, AWS, Anthropic, Telnyx, WhatsApp/Meta und Stripe – jeweils in der tatsächlich gebuchten Vertragsfassung.
- Live-Rechtstexte von mit-frau-schmidt.de und das technische Arbeitsblatt „AVV-Aufgabe MitFrauSchmidt“.

**Rechtlicher Hinweis**

Dieses Dokument ist ein sorgfältig ausgearbeiteter, produktspezifischer Vertragsentwurf. Die rechtliche Belastbarkeit hängt zwingend davon ab, dass die tatsächliche Technik, Providerverträge, Regionen, TOM und Löschprozesse den Zusicherungen entsprechen. Vor Veröffentlichung und automatisiertem Abschluss sollte eine in Deutschland zugelassene, auf IT- und Datenschutzrecht spezialisierte Rechtsanwältin oder ein Rechtsanwalt die finale Produktionsfassung anhand der echten Verträge und Systemkonfiguration freigeben.