

Auftragsverarbeitungsvertrag (AVV)

Dokument 04 des achteiligen Vertragswerks · AKKIVO Line · Fassung V2 · 14. Oktober 2026

Diese Fassung V2 ersetzt die Fassung V1 vom 14. Oktober 2026 für Annahmen ab ihrer Veröffentlichung. Geändert sind ausschließlich die Darstellung des Umsetzungsstands: Die Löschung bei Vertragsende ist seit 14. Oktober 2026 produktiv aktiv; noch offene technische und organisatorische Maßnahmen und ausstehende Bestätigungen sind in den Anlagen 2 bis 5 als offen ausgewiesen, statt die Wirksamkeit dieses Vertrags von ihnen abhängig zu machen. Bereits dokumentierte Annahmen der Fassung V1 bleiben unverändert erhalten.

Zwischen dem in der angenommenen Bestellung bezeichneten Geschäftskunden (nachfolgend „Verantwortlicher“ oder „Kunde“) und Abdulkerim AKKIS, geschäftlich auftretend unter AkkisTech, Freisinger Straße 1, 28215 Bremen, Deutschland (nachfolgend „Auftragsverarbeiter“ oder „Anbieter“). Die verbindliche Identität des Anbieters ergibt sich ausschließlich aus der rechtswirksam angenommenen Bestellung. AKKIVO Line ist die Produktbezeichnung, keine eigene Rechtsperson.

1. Gegenstand, Geltung und Rollen

1.1 Dieser Vertrag konkretisiert die Verarbeitung personenbezogener Daten im Auftrag des Kunden bei Nutzung der bestellten KI-Telefonassistenten einschließlich Anrufannahme, Sprachverarbeitung, Nachrichten und gegebenenfalls Terminanfragen. Er gilt auch für personenbezogene Testdaten während einer Testphase.

1.2 Der Kunde bestimmt Zwecke und wesentliche Mittel der Verarbeitung von Daten seiner Anrufenden und Kontaktpersonen und ist insoweit Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO. Der Anbieter verarbeitet diese Daten nach Art. 4 Nr. 8 und Art. 28 DSGVO ausschließlich als Auftragsverarbeiter, soweit nicht eine gesetzlich eigenständige Rolle besteht.

1.3 Handelt der Kunde seinerseits als Auftragsverarbeiter für einen Dritten, sichert er die erforderliche Beauftragung und Befugnis zur weiteren Unterbeauftragung zu; der Anbieter wird in dieser Verarbeitungskette weiterer Auftragsverarbeiter. Gesetzliche Eigenverantwortung des Anbieters wird dadurch nicht beseitigt.

1.4 Konto-, Vertrags-, Steuer-, Zahlungs-, Betrugspräventions- und gesetzlich erforderliche Telekommunikationsdaten können eigenständigen Verantwortlichkeiten des Anbieters beziehungsweise beteiligter Dienstleister unterliegen. Solche Vorgänge werden nicht allein durch ihre technische Nähe zum Dienst zu Auftragsverarbeitung.

2. Umfang und Dauer

2.1 Art, Zweck, betroffene Personen, Datenarten, Systeme und Vorgänge ergeben sich konkret aus Anlage 1 und der wirksam vereinbarten Leistungsbeschreibung. Der Anbieter darf den Umfang nicht durch eine einseitige Produktbeschreibung erweitern.

2.2 Die Auftragsverarbeitung beginnt erst mit wirksamer Vereinbarung dieses AVV und endet nach Abschluss der Rückgabe und Löschung gemäß Anlage 4, vorbehaltlich gesetzlich vorgeschriebener Aufbewahrung. Eine Fortsetzung der Dienstleistung nach Ende des Hauptvertrags ist damit nicht vereinbart.

3. Dokumentierte Weisungen

3.1 Der Anbieter verarbeitet Auftragsdaten nur aufgrund dokumentierter Weisungen des Kunden, einschließlich dieses AVV, der angenommenen Bestellung und der innerhalb freigegebener Funktionen vorgenommenen Konfiguration, es sei denn, Unionsrecht oder mitgliedstaatliches Recht verlangt eine andere Verarbeitung. In diesem Fall informiert er den Kunden vorab, soweit dies rechtlich zulässig ist.

3.2 Weisungen werden durch nachweisbar autorisierte Personen über die in Anlage 5 beschriebenen sicheren Wege erteilt. Mündliche Eilweisungen sind unverzüglich in Textform zu dokumentieren. Der Anbieter überprüft die Berechtigung und kann zweifelhafte Weisungen bis zur Klärung zurückstellen.

3.3 Hält der Anbieter eine Weisung für datenschutzrechtswidrig, unterrichtet er den Kunden unverzüglich und setzt deren Umsetzung aus, soweit erforderlich. Er dokumentiert die Prüfung und ermöglicht eine rechtmäßige Alternative. Eine generelle fachliche oder rechtliche Freistellung des Anbieters folgt daraus nicht.

4. Vertraulichkeit und Zugriffsberechtigung

4.1 Der Anbieter stellt sicher, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; die Verpflichtung gilt über das Beschäftigungsende hinaus. Zugriffe werden nach Aufgabenbezug begrenzt, erteilt, regelmäßig überprüft und bei Wegfall entzogen.

4.2 Personenbezogene Daten dürfen nicht zu allgemeinen Modelltrainings-, Benchmarking- oder Produktverbesserungszwecken des Anbieters oder eines Unterauftragsverarbeiters verwendet werden, sofern hierfür nicht eine eigenständige, nachweisbar rechtmäßige und ausdrücklich vereinbarte Grundlage besteht. Eine bloße Anbieter-StandardEinstellung ersetzt keine solche Vereinbarung.

5. Sicherheit der Verarbeitung

5.1 Der Anbieter trifft nach Art. 32 DSGVO angemessene technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie von Art, Umfang, Umständen und Zwecken der Verarbeitung und des Risikos für betroffene Personen. Anlage 2 beschreibt die hierfür geschuldeten Kontrollen, den technisch festgestellten Umsetzungsstand und die noch offenen Maßnahmen.

5.2 Änderungen von Schutzmaßnahmen sind zulässig, wenn das Schutzniveau nicht unterschritten wird. Wesentliche risikorelevante Änderungen werden dokumentiert und dem Kunden in geeigneter Form mitgeteilt. Sicherheitszusagen eines Drittanbieters ersetzen keine Bewertung des Gesamtdienstes.

5.3 Der Anbieter sorgt für geeignete Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit seiner Maßnahmen sowie für Wiederherstellungs- und Incident-Response-Verfahren entsprechend dem festgestellten Risiko.

6. Unterauftragsverarbeiter

6.1 Der Kunde erteilt eine allgemeine Genehmigung nur für die in der bei Vertragsschluss verbindlich bezeichneten Fassung der Anlage 3 konkret aufgeführten Unterauftragsverarbeiter und Verarbeitungsvorgänge. Ohne vollständige Anlage 3 darf diese Genehmigung nicht als Freigabe unbestimmter Anbieter verstanden werden.

6.2 Der Anbieter informiert über beabsichtigte Hinzunahmen oder Ersetzungen grundsätzlich mindestens 30 Kalendertage vor deren Zugriff auf Auftragsdaten in Textform und erläutert Identität, Zweck, Datenarten, Orte und Transfergrundlage. Der Kunde kann innerhalb dieses Zeitraums aus sachlichen datenschutzrechtlichen Gründen widersprechen.

6.3 Bei Widerspruch prüfen die Parteien eine geeignete Alternative, Konfiguration oder Abhilfe. Ist eine rechtmäßige Fortsetzung des betroffenen Leistungsteils nicht möglich, kann der Kunde diesen ohne zusätzliche Kündigungsstrafe beenden; bereits gezahlte Entgelte für nicht erbrachte Leistungen sind nach Hauptvertrag und Gesetz abzurechnen. Zwingende Sofortmaßnahmen zum Schutz von Daten bleiben möglich, sind aber unverzüglich zu erläutern.

6.4 Der Anbieter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der im Wesentlichen dieselben Datenschutzpflichten einschließlich geeigneter TOM, Hilfe, Löschung und Nachweisen auferlegt. Er bleibt gegenüber dem Kunden für die Erfüllung der Datenschutzpflichten seiner Unterauftragsverarbeiter verantwortlich (Art. 28 Abs. 4 DSGVO).

7. Drittlandübermittlungen

7.1 Zugriff, Offenlegung oder sonstige Übermittlung personenbezogener Auftragsdaten in Drittländer, einschließlich administrativen Fernzugriffs, ist nur bei dokumentierter Rechtsgrundlage nach Kapitel V DSGVO und unter Beachtung der Weisungen zulässig. Anlage 3 dokumentiert Orte, Empfänger, gegebenenfalls Angemessenheitsbeschluss, Standardvertragsklauseln, Modul und ergänzende Maßnahmen.

7.2 Ein US-Sitz des Anbieters allein beweist weder eine konkrete Übermittlung noch deren Zulässigkeit. Ein EU-Hostingstandort schließt Fernzugriff oder weitere Übermittlungen nicht aus. Die Parteien prüfen erforderlichenfalls Transfer Impact Assessment und wirksame zusätzliche Schutzmaßnahmen.

7.3 Die Standardvertragsklauseln werden, soweit erforderlich, gesondert wirksam abgeschlossen und mit zutreffenden Anhängen ausgefüllt; dieser AVV ersetzt sie nicht. Deren eigene Vorrang- und Betroffenenrechte bleiben unberührt.

8. Betroffenenrechte und Informationspflichten

8.1 Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen durch geeignete technische und organisatorische Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und gegebenenfalls Entscheidungen nach Art. 22 DSGVO.

8.2 An den Anbieter gerichtete Anfragen zu Auftragsdaten leitet er ohne unnötige Verzögerung an den Kunden weiter, soweit zulässig; er beantwortet sie nicht eigenmächtig inhaltlich, außer auf dokumentierte Weisung oder aufgrund zwingenden Rechts. Der Kunde bleibt für die rechtliche Beurteilung und fristgerechte Antwort verantwortlich, der Anbieter für seine Unterstützungsleistung.

8.3 Die Transparenz über den KI-Einsatz, Datenschutzinformationen und eine etwa erforderliche Einwilligung in eine Gesprächsaufzeichnung sind voneinander zu unterscheiden. Eine AVV ersetzt keine Information oder Einwilligung der anrufenden Person.

9. Datenschutzverletzungen

9.1 Der Anbieter meldet dem Kunden eine Verletzung des Schutzes personenbezogener Auftragsdaten unverzüglich nach Bekanntwerden, ohne eine vollständige Ursachenanalyse abzuwarten. Die 72-Stunden-Frist aus Art. 33 Abs. 1 DSGVO betrifft grundsätzlich die Meldung des Verantwortlichen an die Aufsichtsbehörde und ist keine pauschale Wartefrist des Auftragsverarbeiters.

9.2 Die erste Meldung enthält soweit bekannt Art des Vorfalls, betroffene Systeme und Datenkategorien, betroffene Personen und ungefähre Zahl, mögliche Folgen, ergriffene beziehungsweise geplante Maßnahmen, Kontakt und Zeitpunkt. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

9.3 Der Anbieter sichert relevante Beweise verhältnismäßig, unterstützt Eingrenzung und Abhilfe, dokumentiert den Vorfall und kooperiert bei behördlicher Meldung und Betroffenenbenachrichtigung. Er darf notwendige Sicherheitsmaßnahmen nicht von einer gesonderten kostenpflichtigen Beauftragung abhängig machen.

10. Unterstützung nach Art. 32 bis 36 DSGVO

10.1 Der Anbieter unterstützt den Kunden unter Berücksichtigung der Verarbeitung und der ihm verfügbaren Informationen bei Sicherheit, Meldung von Datenschutzverletzungen, Benachrichtigung Betroffener, Datenschutz-Folgenabschätzung und gegebenenfalls vorheriger Konsultation der Aufsichtsbehörde.

10.2 Die Unterstützung umfasst sachlich erforderliche technische Informationen zu Datenflüssen, eingesetzten Dienstleistern, Schutzmaßnahmen und Risiken. Geschäftsgeheimnisse und Sicherheitsinteressen können durch angemessene Vertraulichkeitsmaßnahmen geschützt werden, dürfen die Pflichtunterstützung jedoch nicht leerlaufen lassen.

11. Nachweise und Kontrollen

11.1 Der Anbieter stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht und unterstützt Überprüfungen einschließlich Inspektionen durch den Kunden oder einen von ihm beauftragten Prüfer.

11.2 Zur Vermeidung unnötiger Betriebs- und Sicherheitsrisiken sollen zunächst geeignete Dokumentation, Prüfberichte und Remote-Gespräche genutzt werden. Diese Mittel ersetzen bei begründetem Bedarf kein gesetzlich gebotenes Audit oder eine Vor-Ort-Inspektion.

11.3 Prüfungen erfolgen mit angemessener Vorankündigung während üblicher Betriebszeiten, soweit kein dringender Anlass besteht; Schutz fremder Kundendaten, Geheimhaltung und Sicherheit sind zu wahren. Der Anbieter darf keine unangemessenen Gebühren oder Bedingungen festlegen, die zwingende Nachweis- und Kontrollrechte praktisch vereiteln.

12. Rückgabe, Löschung und Vertragsende

12.1 Nach Ende der Verarbeitung löscht oder gibt der Anbieter nach Wahl des Kunden alle personenbezogenen Auftragsdaten zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht. Wahl, Übergabeformat, Zeitpunkt, Backup-Behandlung und Nachweis richten sich nach Anlage 4.

12.2 Gesetzlich aufzubewahrende Daten werden auf den erforderlichen Umfang beschränkt, von produktiver Nutzung getrennt und nach Wegfall der Pflicht gelöscht. Backups sind nicht unbegrenzt ausgenommen; bis zur turnusmäßigen Löschung sind sie geschützt und dürfen nur zweckgebunden zur Wiederherstellung verwendet werden.

12.3 Der Anbieter weist Unterauftragsverarbeiter zur entsprechenden Löschung oder Rückgabe an und bestätigt die Umsetzung in angemessener, nachvollziehbarer Form. Die Quarantäne einer freigegebenen Rufnummer nach Dokument 03 ist keine Aufbewahrungsfrist für Gesprächsinhalte.

13. Dokumentation und Zusammenarbeit

13.1 Jede Partei führt die gesetzlich erforderlichen Verzeichnisse und Dokumentationen für ihre Rolle. Der Anbieter unterstützt den Kunden mit den für dessen Dokumentation erforderlichen Angaben zu Verarbeitung, Empfängern, Orten und Sicherheitsmaßnahmen.

13.2 Wesentliche Änderungen an Datenflüssen, Unterauftragsverarbeitern, Schutzmaßnahmen oder Aufbewahrung werden vor ihrer datenschutzrechtlich relevanten Umsetzung nachvollziehbar dokumentiert. Nicht freigegebene neue Zwecke sind nicht durch bloße Änderung einer Website zulässig.

14. Haftung und Rechte Dritter

14.1 Die gesetzliche Haftung der Parteien, insbesondere nach Art. 82 DSGVO, und die Rechte betroffener Personen bleiben unberührt. Die interne Verantwortungsverteilung folgt dem jeweiligen tatsächlichen Pflichtverstoß und dem anwendbaren Recht; keine Partei wird allein durch die Rollenbezeichnung pauschal von eigener Verantwortung befreit.

14.2 Die Haftungsregelung in Dokument 01 Ziffer 18 einschließlich der Ausnahmen für Vorsatz, grobe Fahrlässigkeit, Verletzung von Leben, Körper oder Gesundheit und zwingende gesetzliche Haftung wird durch diesen AVV nicht verschärft oder eingeschränkt.

15. Rangfolge, Änderungen und Schlussbestimmungen

15.1 Zwingendes Recht, Individualabreden gemäß § 305b BGB und vorrangige Regelungen wirksam vereinbarter EU-Standardvertragsklauseln bleiben unberührt. Für den Schutz personenbezogener Auftragsdaten hat dieser AVV einschließlich seiner Anlagen Vorrang vor widersprechenden Regelungen in Bestellung, Dokument 01, 02 und 03 sowie den übrigen Vertragsunterlagen.

15.2 Im Übrigen gilt die Rangfolge aus Dokument 01 Ziffer 2. Dieser AVV schafft keine zusätzlichen kostenpflichtigen Leistungsfunktionen, keinen neuen Tarif und keine eigenständige Mindestvertragslaufzeit.

15.3 Änderungen dieses AVV bedürfen einer nachweisbaren Vereinbarung in Textform, soweit gesetzlich zulässig. Eine spätere Veröffentlichung geänderter Anlagen allein bewirkt keine automatische Änderung bestehender Weisungen oder Berechtigungen.

Anlage 1 — Beschreibung der Verarbeitung

Diese Anlage konkretisiert Art. 28 Abs. 3 DSGVO. Maßgeblich ist nur der tatsächlich bestellte und freigeschaltete Funktionsumfang. Eine Beschreibung einer möglichen Verarbeitung ist keine Zusage einer nicht bestellten Funktion.

Vorgang / Zweck	Daten und Betroffene	Verarbeitung / Abgrenzung
Anrufannahme und Live-Audio	Stimme, Rufnummer soweit übermittelt, Gesprächsinhalte; Anrufende und gegebenenfalls genannte Dritte	Empfang, Echtzeitübertragung, Spracherkennung und Antwortausgabe; Live-Stream ist keine automatisch vereinbarte dauerhafte Tonaufzeichnung.
Sprachtranskription	Gesprochene Inhalte, Namen, Kontaktdaten; Anrufende	Temporäre Verarbeitung für Erkennung, Dialogsteuerung und vereinbarte Nachbearbeitung. Das schriftliche Gesprächsprotokoll wird im Kundenportal bereitgestellt und nach Anlage 4 gelöscht.
Dialog und KI-Antwort	Transkriptsegmente, Kontext, vom Kunden freigegebene Wissensinhalte	Übermittlung erforderlicher Ausschnitte an vereinbarte Modelle; Antwortgenerierung; keine pauschale Freigabe für Modelltraining.
Nachrichten und Rückruffbitten	Name, Kontakt, Nachricht, Bestätigungsstatus; Anrufende	Erfassung, Bestätigung, Ablage und vereinbarte Zustellung; Versand ist nicht automatisch Zustellung oder Kenntnisnahme. Bei aktivierter E-Mail-Benachrichtigung wird der Nachrichteninhalte per E-Mail an den Kunden übermittelt.
Terminanfragen	Wunschtermin, Name, Erreichbarkeit, gegebenenfalls Kalenderreferenz	Aufnahme und gegebenenfalls ausdrücklich freigegebene Kalenderaktion; Anfrage und erfolgreiche Buchung sind getrennt.
Kontaktverzeichnis	Name, Telefonnummer, gegebenenfalls Titel; Kontakte	Mandantenbezogene Speicherung und Wiedererkennung nur nach aktivierter Funktion und vorgesehenem Bestätigungsverfahren.
Betrieb und Nachvollziehbarkeit	Verbindungskennungen, Zeitpunkte, technische Status, Fehlercodes; Anrufende und Administratoren	Technischer Betrieb, Fehlerbehebung und Sicherheit; eigene gesetzliche Telekommunikationsverarbeitung ist gesondert abzugrenzen.
Kundenwissen und Einstellungen	Unternehmensinformationen, Mitarbeitendenkontakte, ggf. personenbezogene Wissensinhalte	Aufbereitung und Bereitstellung für die freigegebenen Gesprächsantworten.
Tonaufzeichnung, falls gesondert aktiviert	Audioaufnahme, Stimme, Inhalt	Nicht Bestandteil der bloßen Live-Sprachverarbeitung; nur bei tatsächlich angebotener, vereinbarter und rechtmäßig aktivierter Funktion.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Berufsgeheimnisse sind nicht pauschal freigegeben. Ihre Verarbeitung bedarf einer konkret dokumentierten Zweck- und Risikoprüfung, erforderlicher Rechtsgrundlagen, angemessener Schutzmaßnahmen und gegebenenfalls ergänzender Vereinbarungen. Der Kunde soll nicht erforderliche sensible Angaben aus Gesprächsvorgaben fernhalten; der Anbieter hat technische Schutzpflichten im eigenen Bereich.

Dauer: Für die Laufzeit der beauftragten Funktion zuzüglich des nach Anlage 4 zulässigen Rückgabe- und Löschprozesses. Die konkreten Datenfristen und ihr Umsetzungsstand ergeben sich aus Anlage 4.

Anlage 2 — Technische und organisatorische Maßnahmen (TOM)

Die nachstehenden Anforderungen sind vertragliche Mindestkontrollziele, keine Behauptung einer bereits geprüften Implementierung. Welche Ausprägungen technisch festgestellt sind und welche zum Stand dieser Fassung noch offen sind, weist Ziffer 2.13 aus. Nicht nachgewiesene Maßnahmen dürfen nicht als bestehende Sicherheitsfunktion beworben werden.

2.1 Zutritts- und Gerätesicherheit

Berechtigte Administration; gesicherte Arbeitsgeräte; Sperrung und Entzug bei Ausscheiden; angemessene physische Sicherheit der eingesetzten Rechenzentren.

2.2 Identitäts- und Zugriffsmanagement

Personengebundene Administrationszugänge, rollenbasierte Rechte, Least Privilege, kontrollierte privilegierte Zugriffe und regelmäßige Berechtigungsprüfung.

2.3 Mandantentrennung

Kundenbezogene Zuordnung und serverseitige Berechtigungsprüfung für Gesprächsdaten, Kontakte, Kalender, Wissensinhalte und Nummern; Tests gegen mandantenübergreifenden Zugriff.

2.4 Transport und Speicherung

Schutz von Übertragungswegen und gespeicherten Daten entsprechend Risiko; sichere Behandlung temporärer Audiodaten; Schlüsselverwaltung getrennt von Anwendungsgeheimnissen.

2.5 Geheimnisse und Konfiguration

Geschützte Verwaltung von API-Schlüsseln, Tokens und Zugangsdaten; keine Aufnahme in öffentliche Repositories oder Gesprächsprompts; Rotation und Widerruf nach Anlass.

2.6 Protokollierung und Monitoring

Risikoadäquate Erkennung sicherheitsrelevanter Ereignisse, begrenzter Log-Zugriff, Vermeidung unnötiger Gesprächsinhalte in Logs, nachvollziehbare Incident-Triage.

2.7 Backup und Wiederherstellung

Definierter Sicherungsumfang, kontrollierte Zugriffe, regelmäßige Wiederherstellungsprüfungen und dokumentierter Umgang mit gelöschten Daten in Backups.

2.8 Löschung und Datenlebenszyklus

Datenkategorienbezogene Aufbewahrungsregeln, Löschereignisse, Vererbung an Unterauftragsverarbeiter und Schutz nicht unmittelbar löschbarer Sicherungen.

2.9 Entwicklung und Änderungen

Getrennte Berechtigungen für Entwicklung und Produktion, Codeprüfung, Abhängigkeitenpflege, Sicherheitsupdates, Freigabe und Rückrollplanung.

2.10 Personal und Dienstleister

Vertraulichkeitsbindung, bedarfsgerechte Sensibilisierung, Zugangsentzug, vertragliche Sicherheitsverpflichtungen für Unterauftragsverarbeiter.

2.11 Incident Response

Erkennung, Klassifizierung, Eindämmung, Beweissicherung, Kundennachricht und Nachbereitung nach AVV Ziffer 9.

2.12 Regelmäßige Wirksamkeitsprüfung

Risikobasierte Überprüfung der Maßnahmen, Schwachstellenbehandlung und Dokumentation wesentlicher Abweichungen und Korrekturen.

2.13 Technisch festgestellter Umsetzungsstand

Am 14. Oktober 2026 wurden anhand von Quellcode und Konfiguration der eingesetzten Systeme folgende Maßnahmen festgestellt: serverseitige Prüfung der Zuordnung von Daten zum jeweiligen Kundenkonto bei Zugriffen über das Kundenportal und die internen Schnittstellen; TLS-verschlüsselte Übertragung zwischen Nutzern und Kundenportal; verschlüsselte Speicherung hinterlegter Zugangsdaten für Telefonie- und Integrationsdienste; signierte, zeitlich begrenzte Sitzungsnachweise für die Übergabe von Gesprächsdaten zwischen Sprachverarbeitung und Plattform; standardmäßig deaktivierte Protokollierung von Gesprächsinhalten in der Sprachverarbeitung; Begrenzung von Anmeldeversuchen; Prüfung hochgeladener Wissensdokumente auf Schadsoftware vor der Verarbeitung; automatisierte Löschung von Gesprächsprotokollen, Aktivitätseinträgen und Nachrichten nach Anlage 4.

Zum Stand dieser Fassung nicht umgesetzt beziehungsweise nicht technisch nachgewiesen sind insbesondere: dokumentierte Wiederherstellungstests, Verschlüsselung und externe Kopie der Sicherungen, eine Altersgrenze für Server- und Container-Protokolle sowie die Dokumentation von Standort und physischer Sicherung der Serverinfrastruktur. Eine Datenträgerverschlüsselung des Servers besteht derzeit nicht. Seit 14. Oktober 2026 werden die Datenbanken täglich gesichert; automatische Sicherungen werden nach 14 Tagen gelöscht (festgestellt am 14. Oktober 2026).

Offene Maßnahmen gelten bis zu ihrer Umsetzung nicht als bestehende Sicherheitsfunktion. Ihre Umsetzung wird in einer neuen Fassung dieser Anlage dokumentiert und dem Kunden nach AVV Ziffer 5.2 mitgeteilt. Weitere technische Parameter (einschließlich Authentisierungsverfahren, Verschlüsselung, Regionen, Wiederherstellungsziele und Logfristen) stellt der Anbieter im Rahmen von AVV Ziffer 11 auf Anfrage zur Verfügung. Zertifizierungen wie ISO 27001 oder SOC 2 werden nicht als vorhandene AKKIVO-Zertifizierungen zugesichert.

Anlage 3 — Unterauftragsverarbeiter und Verarbeitungsorte

Die folgenden Anbieter sind als eingesetzte Dienste vom Anbieter benannt. Ihre konkrete vertragsführende Gesellschaft, vertragliche Rolle, Region und Übermittlungskonfiguration sind zum Stand dieser Fassung nicht für jeden Dienst anhand der jeweiligen Kundenkonten und Verträge abschließend bestätigt; ausstehende Bestätigungen sind in der Tabelle als ausstehend gekennzeichnet und werden in einer neuen Fassung dieser Anlage nachgetragen. Die öffentliche Anbieter-DPA allein belegt diese Konfiguration nicht. Die Plattform wird nach dem am 14. Oktober 2026 festgestellten technischen Stand auf einer vom Anbieter selbst administrierten Serverinfrastruktur betrieben; ein externer Hosting-Dienstleister mit Zugriff auf Auftragsdaten ist danach nicht eingebunden.

Dienst / öffentlich dokumentierte Organisation	Zweck / mögliche Daten	Datenschutzrechtliche Einordnung
Twilio (vertragsführende Twilio-Gesellschaft gemäß AKKIVO-Konto)	Telefonie, Anrufweiterleitung, Rufnummern, Verbindungsmetadaten und Live-Audio; über Twilio ConversationRelay zusätzlich Spracherkennung und Sprachausgabe	Für kundenbeauftragte Kommunikationsverarbeitung Unterauftragsverarbeiter; eigene gesetzliche Telekommunikationsrollen gesondert. Twilio bindet für ConversationRelay je nach Sprachprofil Google oder Deepgram (Spracherkennung) und ElevenLabs (Sprachausgabe) ein; deren Einordnung nach dem Twilio-Vertrag sowie Regionen/Edge und DPA: Bestätigung ausstehend.
Deepgram (vertragsführende Deepgram-Gesellschaft gemäß AKKIVO-Konto, soweit direkt angebunden)	Spracherkennung; Audio und Transkript	Einbindung über Twilio ConversationRelay sowie technisch vorhandene direkte Anbindung für einen alternativen Sprachpfad. Produktiver Einsatz der direkten Anbindung, Datenverwendung zu Modellverbesserung und Opt-out/DPA-Konfiguration: Verifizierung ausstehend.
ElevenLabs (über Twilio ConversationRelay)	Sprachausgabe; vom Assistenten erzeugter Antworttext, der personenbezogene Angaben wie Namen enthalten kann	Einbindung über Twilio; vertragliche Rolle, Region und Datenverwendung: Bestätigung ausstehend.
Google (Spracherkennung über Twilio ConversationRelay, je nach Sprachprofil)	Spracherkennung; Audio und Transkript	Einbindung über Twilio; vertragliche Rolle, Region und Datenverwendung: Bestätigung ausstehend.
OpenAI (vertragsführende OpenAI-Gesellschaft gemäß AKKIVO-API-Vertrag)	LLM-Dialogverarbeitung und Erstellung von Embeddings für Kundenwissen; erforderliche Textsegmente, Kontext und Wissensinhalte	Unterauftragsverarbeiter für beauftragte API-Inhalte; konkrete Modelle, Endpunkte, Aufbewahrung, Region und internationale Transfergrundlage: Prüfung ausstehend.
Cloudflare (vertragsführende Cloudflare-Gesellschaft gemäß AKKIVO-Konto)	DNS, TLS-Terminierung und Tunnel für Kundenportal, Plattformschnittstellen und Telefonie-Verbindungen einschließlich der übertragenen Gesprächsinhalte	Unterauftragsverarbeiter für die Datenübertragung; DPA, Verarbeitungsorte und Transfergrundlage: Bestätigung ausstehend.
Zoho Mail (EU-Dienst; vertragsführende Zoho-Gesellschaft gemäß AKKIVO-Konto)	Versand von Konto- und Benachrichtigungs-E-Mails; bei aktivierter Option Inhalt von Anrufernachrichten, Name und Rückrufnummer	Unterauftragsverarbeiter, soweit Auftragsdaten per E-Mail übermittelt werden; DPA und Speicherung gesendeter Nachrichten: Bestätigung ausstehend.
Stripe (vertragsführende Stripe-Gesellschaft gemäß AKKIVO-Konto)	Zahlung, Abonnement, Rechnung und Betrugsprävention; Vertrags- und	Grundsätzlich nicht pauschal Unterauftragsverarbeiter für

Gesellschaft gemäß AKKIVO-Konto)	Zahlungsdaten	Anrufinhalte. Je Zahlungsfunktion unabhängiger Verantwortlicher und/oder Auftragsverarbeiter für AKKIVO-eigene Daten; getrennte Datenschutzinformation erforderlich.
----------------------------------	---------------	--

Für jeden tatsächlich eingesetzten Auftragsdatenempfänger ergänzt der Anbieter das Unterauftragsverarbeiterverzeichnis um: vollständige juristische Firma, Anschrift, Dienst, Datenkategorien, Rolle, Speicher- und Zugriffsorte, eingesetzte nachgelagerte Unterauftragsverarbeiter, wirksame DPA-Fassung, einschlägiges Kapitel-V-Instrument und Änderungsstand. Hosting, E-Mail, Backups, Fehlertracking und Support sind ebenfalls aufzunehmen, soweit sie Auftragsdaten verarbeiten. Diese Angaben stehen zum Stand dieser Fassung teilweise noch aus; sie werden dem Kunden auf Anfrage und mit der nächsten Fassung dieser Anlage bereitgestellt. Die Genehmigung nach AVV Ziffer 6.1 umfasst die in der Tabelle benannten Dienste ausschließlich für die dort beschriebenen Zwecke und Datenarten.

Änderungen richten sich nach AVV Ziffer 6. Die öffentliche Subprozessorliste des jeweiligen Anbieters kann als ergänzende dynamische Informationsquelle dienen, ersetzt aber nicht die dokumentierte Genehmigung der unmittelbaren AKKIVO-Unterauftragsverarbeiter.

Anlage 4 — Aufbewahrung, Rückgabe und Löschung

Die nachfolgende Matrix gibt die mit dieser Fassung V2 vereinbarten Fristen und den am 14. Oktober 2026 anhand von Quellcode, Konfiguration und Tests festgestellten Umsetzungsstand wieder. Der Stand ist je Kategorie als „Umgesetzt“, „Konfiguration erforderlich“, „Noch nicht umgesetzt“ oder „Rechtliche Prüfung erforderlich“ ausgewiesen; dieser AVV enthält bewusst keine erfundenen Tageszahlen. Als „Noch nicht umgesetzt“, „Konfiguration erforderlich“ oder „Rechtliche Prüfung erforderlich“ gekennzeichnete Punkte sind zum Stand dieser Fassung offen und werden nicht als umgesetzt zugesagt. Ihre Erledigung dokumentiert der Anbieter in einer neuen Fassung dieser Anlage. Bis dahin gelten für die betroffenen Kategorien die hier ausgewiesenen Angaben und im Übrigen AVV Ziffer 12.

Datenkategorie und Speicherort	Freigegebene Frist und Umsetzungsstand	Vertragsende, Sicherungen und offene Punkte
Live-Audio und Streaming-Puffer (Twilio und eingebundene Sprachdienste)	Keine Speicherung von Audiodaten in den Systemen des Anbieters; Verarbeitung nur während des laufenden Gesprächs. Stand: Umgesetzt.	Zwischenspeicherung bei Twilio und den eingebundenen Sprachdiensten richtet sich nach deren Konfiguration. Stand: Konfiguration erforderlich; Bestätigung der Anbieterkonfiguration ausstehend.
Dauerhafte Audioaufzeichnung	In V1 nicht angeboten; eine Aufzeichnungsfunktion ist technisch nicht implementiert.	Entfällt. Eine spätere Einführung erfordert eine Ergänzung dieser Anlage.
Gesprächsprotokolle (Transkripte) mit Rufnummer, Sprache und Dauer (Plattformdatenbank)	Frist: 90 Tage nach Speicherung. Automatische Löschung durch einen stündlichen Löschlauf; dabei werden Rufnummer und Protokollverweis im zugehörigen Aktivitätseintrag entfernt. Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv.	Bei Vertragsende läuft die 90-Tage-Frist weiter. Sicherungen: siehe unten.
Aktivitätseinträge mit Kurzzusammenfassung, erkanntem Anliegen und Aktionsdaten (Plattformdatenbank)	Frist: 90 Tage nach dem Gesprächszeitpunkt. Automatische Löschung im selben Löschlauf einschließlich zugehöriger Hinweise im Kundenportal. Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv.	Kopien in Benachrichtigungs- und zugestellten Übermittlungsdatensätzen: Schwärzung nach 90 Tagen. Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv. Nicht zugestellte Übermittlungen (Fehlerablage) werden nicht geschwärzt.
Nachrichten und Rückruffbitten mit Name, Rückrufnummer und Inhalt (Plattformdatenbank); E-Mail-Benachrichtigungen an den Kunden	Frist: 90 Tage nach Speicherung. Automatische Löschung im selben Löschlauf. Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv.	Zugestellte E-Mails liegen im Postfach des Kunden und unterliegen dessen Kontrolle. Speicherung gesendeter Nachrichten beim E-Mail-Dienstleister: Konfiguration erforderlich; eine Aufbewahrungsdauer ist dort zum Stand dieser Fassung nicht festgelegt.
Termine mit Name, Rufnummer, Zeitpunkt und Notiz (Plattformdatenbank; gegebenenfalls angebundener Kalender des Kunden)	Frist: bis zum Vertragsende. Der Kunde kann Termine im Kundenportal stornieren; eine Löschfunktion für einzelne Termine besteht nicht. Stand: Löschung bei Vertragsende siehe rechte Spalte.	Löschung 30 Tage nach dem tatsächlichen Vertragsende (siehe Konto-, Workspace- und Vertragsdaten). Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv. Einträge im angebundenen Kalender verwaltet der Kunde in seinem System (Dokument 02 Ziffer 22.2).
Kontakte mit Name, Rufnummer und Anrede (Datenbank des Kundenportals)	Frist: bis zur Löschung durch den Kunden oder bis zum Vertragsende. Der Kunde kann einzelne Kontakte im Kundenportal löschen. Stand: Umgesetzt.	Löschung 30 Tage nach dem tatsächlichen Vertragsende (siehe Konto-, Workspace- und Vertragsdaten). Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv.
Kundenwissen: hochgeladene	Frist: bis zur Löschung durch den	Löschung 30 Tage nach dem

Dokumente, importierte Webseiten sowie daraus erzeugte Textabschnitte und Embeddings (Wissensdienst)	Kunden oder bis zum Vertragsende. Der Kunde kann Dokumente und Webseitenquellen im Kundenportal entfernen; zugehörige Textabschnitte und Embeddings werden mitgelöscht. Stand: Umgesetzt.	tatsächlichen Vertragsende einschließlich gespeicherter Dateien, Textabschnitte und Embeddings (siehe Konto-, Workspace- und Vertragsdaten). Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv.
Konto-, Workspace- und Vertragsdaten (Datenbank des Kundenportals, Plattformdatenbank)	Frist: kontrollierte Löschung 30 Tage nach dem tatsächlichen Ende des letzten Leistungsrechts (bezahltes Abonnement einschließlich Nachfrist oder Testzeitraum). Eine Kündigung oder ein Zahlungsausfall allein löst keine Löschung aus; ein neues Leistungsrecht innerhalb der 30 Tage hebt die geplante Löschung auf. Gelöscht werden in der Plattform Gespräche, Nachrichten, Termine, Kundenwissen, Assistenten- und Kalenderkonfiguration einschließlich gespeicherter Kalender-Zugangsdaten (ohne Widerruf beim Kalenderanbieter) sowie Dateien, im Kundenportal Kontakte, Onboarding-, Aktivitäts- und Mitgliedschaftsdaten. Kontaktangaben im Kundenprofil und Absenderangaben von Supportanfragen werden anonymisiert; der Workspace wird archiviert. Stand: Umgesetzt und seit 14. Oktober 2026 produktiv aktiv.	Überwiegend eigenverantwortliche Verarbeitung des Anbieters (Ziffer 1.4); Information nach Dokument 05. Erhalten bleiben Rechnungs-, Zahlungs-, Abonnement- und Nutzungsnachweise, Vertragsannahme- und Einwilligungsnachweise, Supportanfragen ohne Absenderangaben sowie zur Missbrauchsvermeidung die bei einem Test verwendete Rufnummer. Das Zugangskonto (Name, E-Mail-Adresse) bleibt bestehen; seine Löschung ist nicht automatisiert. Aufbewahrungsfristen von Vertrags- und Rechnungsdaten: Rechtliche Prüfung erforderlich.
Verbindungs- und Abrechnungsmetadaten (Anruferkennung, Zeitpunkt, Dauer)	Aufbewahrung als Abrechnungsnachweis; keine automatische Löschung.	Fristen nach handels- und steuerrechtlichen Aufbewahrungspflichten: Rechtliche Prüfung erforderlich.
Technische Protokolle (Anwendungs-, Container-, Proxy- und Telefonie-Logs)	Ziel: höchstens 30 Tage. Gesprächsinhalte werden in der Sprachverarbeitung standardmäßig nicht protokolliert. Container-Protokolle von Plattform und Kundenportal sind seit 14. Oktober 2026 in der Größe begrenzt (je Container höchstens 100 MB beziehungsweise 30 MB); für die Sprachverarbeitung ist die Begrenzung vorbereitet und wird mit ihrer nächsten Bereitstellung wirksam. Stand: Konfiguration erforderlich.	Eine Altersgrenze von 30 Tagen ist zum Stand dieser Fassung nicht eingerichtet; bis zum Erreichen der Größenbegrenzung können Protokolle älter als 30 Tage sein. Sicherheitsrelevante Protokolle, die für einen konkreten Vorfall benötigt werden, können für dessen Aufklärung länger aufbewahrt werden.
Sicherungen (Backups)	Seit 14. Oktober 2026 werden die Datenbanken von Plattform und Kundenportal täglich automatisch gesichert und geprüft; automatische Sicherungen werden nach 14 Tagen gelöscht. Die Sicherungen liegen auf demselben Server. Vor dem 14. Oktober 2026 erstellte manuelle Sicherungen haben keine festgelegte Löschfrist. Stand: Umgesetzt (tägliche Sicherung und Rotation).	Eine Verschlüsselung und eine externe Kopie der Sicherungen bestehen zum Stand dieser Fassung nicht; die manuellen Altsicherungen sind nicht gelöscht. Stand: Konfiguration erforderlich. Bis zur Rotation (höchstens 14 Tage) enthalten automatische Sicherungen auch bereits gelöschte Daten; sie werden nur zur Wiederherstellung verwendet.
Gesetzlich aufzubewahrende Daten	Aufbewahrung bis zum Ende der	Zweckbindung, Einschränkung und

jeweils einschlägigen Rechtsfrist.	nachfolgende Löschung; keine pauschale Ausnahme. Rechtliche Prüfung erforderlich.
------------------------------------	---

Auf Wahl des Kunden werden Auftragsdaten vor der endgültigen Löschung in einem strukturierten, gängigen, maschinenlesbaren Format zurückgegeben, soweit dies technisch vorhanden und für die Verarbeitung sachgerecht ist. Sichere Übergabe, Identitätsprüfung, Exportumfang, Fristen und Löschbestätigung werden vor Vertragsende abgestimmt; gesetzliche Betroffenenrechte bleiben unabhängig von einer optionalen Exportfunktion bestehen.

Der Anbieter unterrichtet die Unterauftragsverarbeiter über die Beendigung, dokumentiert deren Lösch- oder Rückgabebestätigungen und stellt dem Kunden eine angemessene Abschlussbestätigung bereit. Eine 90-tägige oder andere Rufnummernquarantäne ist keine Frist für Gesprächsdaten.

Anlage 5 — Weisungen und Sicherheitskommunikation

5.1 Zuständigkeiten

Kundenseitig sind die in der angenommenen Bestellung beziehungsweise der gesicherten Kundenadministration nachweisbar autorisierten Personen weisungsbefugt. Anbieterintern bearbeitet die benannte Datenschutz-/Sicherheitsfunktion die Weisung und bestätigt die Zuständigkeit. Die operative Kontaktstelle des Anbieters ist am Ende dieser Anlage benannt. Eine dokumentierte Vertretungsregelung ist zum Stand dieser Fassung noch festzulegen.

5.2 Kanäle und Authentisierung

Reguläre Weisungen werden über eine dafür freigegebene, nachvollziehbare Kundenkommunikation in Textform übermittelt. Als Meldekanal für dringende Sicherheitsvorfälle dient der am Ende dieser Anlage benannte Kontakt. Die bloße Veröffentlichung einer allgemeinen E-Mail-Adresse ist keine Zusage eines durchgehend besetzten 24/7-Kanals.

5.3 Weisungsregister

Für wesentliche Weisungen sind Datum, Kunde/Workspace, autorisierte Person, Gegenstand, betroffene Daten, Empfang, Prüfung, Umsetzung und Abschluss nachvollziehbar festzuhalten. Das Register darf selbst keine unnötigen Gesprächsinhalte enthalten.

5.4 Vorfallmeldungen

Sicherheitsmeldungen werden an die vereinbarten Kontakte übermittelt und enthalten soweit bekannt Zeitpunkt, Umfang, Kategorien, mögliche Folgen, Sofortmaßnahmen, offenen Informationsbedarf und nächste Aktualisierung. Zusätzliche Erkenntnisse werden stufenweise nachgereicht; die unverzügliche Erstmeldung wird nicht bis zur vollständigen Klärung verzögert.

5.5 Änderung und Eskalation

Bei unklarer Berechtigung, widersprüchlicher Weisung, fehlgeschlagener Zustellung oder datenschutzrechtlichem Widerspruch erfolgt eine nachvollziehbare Eskalation an die benannten Verantwortlichen. Bis zur Klärung sind risikobegrenzende Maßnahmen zulässig, ohne gesetzliche Unterstützungspflichten auszusetzen.

Kontakt des Anbieters für Weisungen, Meldungen von Datenschutzverletzungen und Sicherheitsvorfälle: support@akkivo.ai. Eine durchgehende Erreichbarkeit (24/7) wird damit nicht zugesagt; Ziffer 5.2 dieser Anlage gilt.