

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 Abs. 1 DSGVO

Auftragsverarbeiter	Felix Oskar Griebeler
Kontakt	felix@kalendria.org
Geltungsbereich	Bereitstellung eines KI-gestützten telefonischen Rezeptionisten (Telefonassistent) für Betriebe des SHK-Handwerks (Sanitär, Heizung, Klima) auf Basis der Plattformen Twilio, Retell AI, n8n und cal.eu (Cal.com) sowie – bei Benachrichtigung per E-Mail – Google Workspace
Stand / Version	10.10.2026 – Version 1.2
Referenzdokument	VVT Absatz 2 (Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters nach Art. 30 Abs. 2 DSGVO)
Einbindung	Anlage 2 zum Auftragsverarbeitungsvertrag (AVV), Version 1.8; wird als gesondertes Dokument bereitgestellt.

1. Einleitung und rechtlicher Rahmen

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM), die zum Schutz personenbezogener Daten im Rahmen der in Auftrag genommenen Verarbeitungstätigkeiten umgesetzt werden. Es dient der Erfüllung der Anforderungen aus Art. 32 Abs. 1 DSGVO sowie der Dokumentationspflicht nach Art. 30 Abs. 2 lit. d DSGVO und wird im VVT Absatz 2 sowie in den Auftragsverarbeitungsverträgen (AVV) mit Auftraggebern in Bezug genommen.

Die Gliederung dieses Dokuments orientiert sich an den von der Datenschutzkonferenz (DSK) veröffentlichten „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO“ (Stand: Februar 2018), die in Ziffer 6.7 bis 6.9 die nach Art. 32 Abs. 1 DSGVO sowie ergänzend zu berücksichtigenden Maßnahmenbereiche aufführen. Die dort genannten neun Kategorien bilden die Struktur dieses Dokuments; die konkreten Maßnahmen wurden individuell für die im Geltungsbereich beschriebene Verarbeitungstätigkeit ermittelt und dokumentiert.

Die Angemessenheit der Maßnahmen wurde unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen festgelegt (Art. 32 Abs. 1 DSGVO). Es wird keine eigene Serverinfrastruktur betrieben; sämtliche Verarbeitung erfolgt über die im Geltungsbereich genannten Cloud-Plattformen (Subunternehmer), deren technische und organisatorische Maßnahmen vertraglich über Data Processing Agreements (DPA) zugesichert sind.

1.1 Eingesetzte Subunternehmer

Die folgenden Subunternehmer kommen im Rahmen der Leistungserbringung zum Einsatz und werden in den nachfolgenden Kategorien referenziert:

Subunternehmer	Funktion	Zertifizierung
Twilio Inc. / Twilio Ireland Ltd.	Rufnummer, Telefonverbindung, Weiterleitung, SMS-Versand	SOC 2 Type II, ISO 27001/17/18, PCI DSS

Subunternehmer	Funktion	Zertifizierung
Retell AI, Inc.	KI-Sprachplattform (Spracherkennung, Sprachmodell, Stimme, Bereinigung der Mitschrift)	SOC 2 Type II (auf Anfrage)
n8n GmbH	Workflow-Orchestrierung, Qualitätsarchiv, Überwachung	SOC 2 Type II
Cal.com, Inc. (cal.eu)	Terminverwaltung (EU-Hosting)	SOC 2 Type II, ISO 27001
Google Ireland Limited (Google Workspace)	Versand von E-Mails an den Auftraggeber (nur bei Benachrichtigung per E-Mail)	SOC 2, ISO 27001/17/18

Microsoft Azure (Spracherkennung), OpenAI (Sprachmodell) und ElevenLabs (Sprachsynthese) sind Sub-Subunternehmer von Retell AI, die von diesem im Rahmen des eigenen Verarbeitungsverhältnisses beauftragt und verantwortet werden; deren technische und organisatorische Maßnahmen sind nicht Gegenstand dieses Dokuments. Gesprächsinhalte werden an keinen weiteren KI-Anbieter übermittelt.

2. Pseudonymisierung personenbezogener Daten

Automatische Bereinigung der Mitschrift durch Retell AI

Nach Abschluss eines Anrufs erkennt Retell AI automatisiert personenbezogene Daten in Mitschrift und Zusammenfassung – einschließlich der Angaben in Funktionsaufrufen – und ersetzt sie durch standardisierte Platzhalter (z. B. „[person name 1]“, „[phone number 1]“, „[address 1]“). Folgende Kategorien sind aktiviert:

- Identitätsinformationen: Name, Geburtsdatum, Kundenkontonummer
- Kontaktinformationen: Adresse, E-Mail-Adresse, Telefonnummer
- Amtliche Identifikatoren: Sozialversicherungsnummer, Reisepass
- Finanzdaten: Kreditkartendaten, Bankkontodaten
- Sicherheitsdaten: Passwörter, PIN
- Gesundheitsdaten: medizinische Identifikationsnummern

Keine dauerhafte Speicherung bei Retell AI

Retell AI ist auf „Basic Attributes Only“ eingestellt: Mitschrift und Aufnahme werden dort nicht dauerhaft gespeichert; der technische Link zur Aufnahme verfällt wenige Minuten nach Gesprächsende. Gespeichert werden nur Verbindungsdaten (7 Tage).

Qualitätsarchiv nur in bereinigter Form

Für die Qualitätssicherung übernimmt n8n ausschließlich die bereinigte Mitschrift, die bereinigte Zusammenfassung, Dauer, Gesprächserfolg und technische Fehler in das Qualitätsarchiv. Liefert Retell AI keine bereinigte Fassung, wird keine Mitschrift bzw. Zusammenfassung gespeichert. Eine Einschätzung der Gesprächsstimmung wird nicht gespeichert. Hat der Anrufer der Aufzeichnung widersprochen, wird nichts archiviert. Die Einträge werden nach 7 Tagen automatisch gelöscht. Angaben außerhalb der genannten Kategorien, etwa vom Anrufer genannte Gesundheitsangaben, werden nicht automatisch entfernt; ob die Bereinigung greift, wird bei der Qualitätsprüfung stichprobenartig kontrolliert (Kategorie 7).

Einordnung der übrigen Subunternehmer

Twilio, n8n (bei den Funktionsaufrufen während des Gesprächs), cal.eu und Google verarbeiten bewusst nicht-pseudonymisierte Daten, da dies für den jeweiligen Zweck (Telefonverbindung, Terminbuchung, Benachrichtigung des Auftraggebers) erforderlich ist; eine Pseudonymisierung wäre an diesen Stellen zweckwidrig und würde die Erfüllung der Leistung verhindern.

3. Verschlüsselung personenbezogener Daten

Verschlüsselung bei den eingesetzten Subunternehmern

Sämtliche im Geltungsbereich genannten Subunternehmer (Twilio, Retell AI, n8n, cal.eu, Google) sichern in ihren jeweiligen Data Processing Agreements die Verschlüsselung personenbezogener Daten sowohl während der Übertragung (in transit) als auch im Ruhezustand (at rest) vertraglich zu.

Eigene Maßnahmen

- Sämtliche API- und Webhook-Verbindungen zwischen den eingesetzten Systemen (Retell AI, n8n, cal.eu, Twilio, Google) erfolgen ausschließlich über verschlüsselte HTTPS/TLS-Verbindungen.
- Die Funktionsaufrufe von Retell AI an n8n sowie die Auslösung des Notschalters sind zusätzlich durch eine Header-Authentifizierung mit einem geheimen Token abgesichert, sodass ausschließlich autorisierte Anfragen die Abläufe auslösen können.
- Die Links zum Wiedereinschalten des Telefonassistenten enthalten ein geheimes Token; die Adressen der übrigen Webhooks (Anrufauswertung, Notweg) sind zufällig gewählt und nicht erratbar.
- Zugangsschlüssel zu den Plattformen (z. B. zum Kalender) liegen ausschließlich in den Zugangsdaten-Speichern der Plattformen und werden nicht in Dokumenten oder Nachrichten weitergegeben.

4. Gewährleistung der Vertraulichkeit und Integrität der Systeme und Dienste

Zugriffsschutz auf eingesetzte Plattformen

- Der Zugriff auf sämtliche Plattform-Accounts erfolgt ausschließlich durch eine einzelne, namentlich festgelegte Person; ein weiterer Personenzugriff besteht nicht.
- Für jede Plattform wird ein langes, zufällig generiertes und einzigartiges Passwort verwendet, verwaltet über einen Passwort-Manager (Apple iCloud-Schlüsselbund).
- Multi-Faktor-Authentifizierung (MFA) über eine Authenticator-App (Google Authenticator) ist aktiviert bei: Twilio, n8n, cal.eu und Google Workspace.
- Bei Retell AI steht MFA bei direkter Anmeldung über die eigene Geschäfts-E-Mail-Domain nicht zur Verfügung (eine MFA-Absicherung wäre nur über einen optionalen, hier bewusst nicht genutzten Google-Konto-Login verfügbar). Als kompensierende Maßnahme wird ein besonders langes, zufällig generiertes, ausschließlich für diesen Account verwendetes Passwort eingesetzt.
- Wiederherstellungs-/Backup-Codes für die MFA-Absicherung werden sowohl digital als auch physisch gesichert aufbewahrt.
- Im Rahmen der monatlichen Sicherheitsüberprüfung (siehe Kategorie 7) wird zusätzlich die Login-Historie der eingesetzten Plattformen eingesehen, um unautorisierte Zugriffe zeitnah erkennen zu können.
- Benachrichtigungen an den Auftragsverarbeiter über Störungen, Überwachung und Löschläufe enthalten keine Anruferdaten.

Endgerätesicherheit

Auf dem zur Verwaltung der Plattformen genutzten Endgerät ist eine vollständige Festplattenverschlüsselung (FileVault) aktiviert.

5. Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste**Plattformseitige Verfügbarkeit**

Die Verfügbarkeit der eingesetzten Cloud-Plattformen wird durch die jeweiligen Anbieter im Rahmen ihrer Service Level Agreements und vertraglichen Zusicherungen sichergestellt. Es wird keine eigene Serverinfrastruktur betrieben.

Mehrstufige Fehlerbehandlung bei Integrationsausfällen

Es wird zwischen zwei Fehlerszenarien unterschieden:

1. Ausfall eines von n8n angesteuerten Dienstes (cal.eu, Twilio oder Google), während n8n selbst funktionsfähig ist: n8n antwortet dem Assistenten mit einer Fehlermeldung. Der Assistent bestätigt dann nichts, was nicht erledigt ist; bei Terminproblemen nimmt er das Anliegen zur Weitergabe auf, sonst bittet er den Anrufer, es später erneut zu versuchen. Ein bereits gebuchter Termin bleibt bestätigt, auch wenn die anschließende Benachrichtigung scheitert.
2. Ausfall von n8n selbst (keine Antwort): Jeder Funktionsaufruf wartet höchstens 20 Sekunden; währenddessen spricht der Assistent einen festen Überbrückungssatz, damit keine Stille entsteht. Bleibt die Antwort aus, wird der Aufruf wie unter 1. als Fehler behandelt; eine automatische Wiederholung findet nicht statt.

In beiden Fällen wird der Anrufer nicht ohne Reaktion gelassen.

Sicherung und Prüfung von Änderungen

Die n8n-Workflows und die Konfiguration der Assistenten in Retell AI werden über die integrierte Versionshistorie der Plattformen gesichert. Änderungen werden vor der Übernahme in den Livebetrieb mit Testanrufen bzw. Testaufrufen geprüft, ohne das produktiv laufende System zu beeinträchtigen.

Automatische Überwachung und Notschalter

Ein stündlicher Prüflauf in n8n wertet für jeden Assistenten das Qualitätsarchiv aus. Eine Erfolgsquote unter 80 % bei mindestens fünf Anrufen in 24 Stunden oder mehr als ein Funktionsfehler in der letzten Stunde lösen den Notschalter aus (höchstens ein Alarm je Assistent in 24 Stunden). Der Notschalter löst die Rufnummer des Assistenten von der Anbindung an die Sprach-KI-Plattform und leitet Anrufe über den Notweg direkt an die vom Auftraggeber benannte Zweitnummer weiter – technisch durch Anpassung der Rufnummer bei Twilio. Auftragsverarbeiter (SMS und E-Mail) und Auftraggeber (SMS) werden automatisch benachrichtigt. Nach Behebung der Störung schaltet der Auftragsverarbeiter den Assistenten über einen gesicherten Link wieder ein; der Auftraggeber wird erneut benachrichtigt.

Notweg bei Ausfall der Sprach-KI-Plattform

Ist Retell AI nicht erreichbar, leitet Twilio eingehende Anrufe automatisch über den Notweg an die Zweitnummer des Auftraggebers weiter; der Auftragsverarbeiter wird per SMS und E-Mail informiert. Ein Schutz vor Anrufschleifen verhindert, dass Anrufe zwischen Zweitnummer und Assistent kreisen. Statusmeldungen von Twilio werden zusätzlich abonniert.

Dokumentiertes Restrisiko

Fallen Twilio oder n8n selbst aus, können Notschalter und Notweg nicht greifen. Diese Fälle liegen außerhalb der eigenen Einflussmöglichkeiten und werden durch die Verfügbarkeitszusagen der Anbieter abgedeckt.

6. Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem Zwischenfall

Versionsverwaltung und Rollback-Fähigkeit

Sowohl n8n als auch Retell AI bieten eine integrierte Versionshistorie der jeweiligen Workflow- bzw. Agent-Konfiguration, über die bei fehlerhaften Updates ein Rollback auf einen vorherigen Stand vorgenommen werden kann.

Test vor dem Livebetrieb

Vor dem Go-Live testet der Auftraggeber seinen Assistenten über eine Testnummer und mit einem Testkalender. Technische Änderungen und inhaltliche Verbesserungen werden vor der Übernahme in den Livebetrieb mit Testanrufen geprüft.

Automatisierte Anrufumleitung bei Systemausfall

Bei einer Störung leiten Notschalter bzw. Notweg die Anrufe automatisch an die Zweitnummer des Auftraggebers weiter (Kategorie 5); eine gesonderte Handlung des Auftraggebers ist hierfür nicht erforderlich.

Dokumentiertes Restrisiko

Zwischen dem Eintritt einer funktionalen oder inhaltlichen Störung und dem Auslösen des Notschalters vergeht bis zu eine Stunde (stündlicher Prüflauf), in der Anrufe weiter vom Assistenten bearbeitet werden. Fallen n8n oder Twilio selbst aus, kann die automatische Umleitung nicht ausgeführt werden; in Twilio verbleiben dann lediglich Verbindungsdaten des eingehenden Anrufs (insbesondere die anrufende Rufnummer), ohne Zuordnung zu Name oder Anliegen. Eine Weitergabe dieser Rufnummer an den Auftraggeber ist keine reguläre, angebotene Maßnahme, sondern ausschließlich auf ausdrückliche, im Einzelfall begründete Anfrage hin möglich.

Keine eigene Anrufaufzeichnung

Eine eigene Aufzeichnung abgeschlossener Anrufe wird nicht geführt; Audioaufnahmen werden nirgends dauerhaft gespeichert.

Verhältnismäßige Reaktion auf Plattform-Störungen

Bei einem geringfügigen, isolierten und nicht öffentlich kommunizierten Vorfall bei einer eingesetzten Plattform wird der betroffene Assistent nicht automatisch offline genommen, da eine vollständige Außerbetriebnahme in solchen Fällen unverhältnismäßig wäre. Bei einer von der jeweiligen Plattform öffentlich kommunizierten Störung wird der betroffene Assistent hingegen über den Notschalter offline genommen; dies gilt einheitlich für alle eingesetzten Plattformen.

Offline-Nahme bei Qualitätsproblemen

Unabhängig von der technischen Verfügbarkeit der eingesetzten Plattformen wird ein Assistent auch dann offline genommen, überarbeitet und mit Testanrufen geprüft, wenn er inhaltlich nicht zufriedenstellend funktioniert (z. B. fehlerhafte oder unpassende Gesprächsführung).

Vorgehen bei Sicherheitsvorfällen (Incident Response)

Im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls wird wie folgt vorgegangen:

1. Sofortmaßnahme: Betroffenen Account-Zugang sperren bzw. Passwort umgehend ändern; betroffenen Assistenten ggf. offline nehmen.
2. Eingrenzung: Prüfen, welche Plattform(en), Tätigkeit(en) und Auftraggeber betroffen sind oder sein könnten.
3. Information: Betroffene Auftraggeber unverzüglich informieren, damit diese ihrerseits ihren Meldepflichten nachkommen können.

4. Dokumentation: Vorfall, Zeitpunkt der Entdeckung und ergriffene Maßnahmen schriftlich festhalten.

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit

Regelmäßige eigene Sicherheitsüberprüfung

Die eigenen Kontosicherheitseinstellungen (MFA-Status, Passwörter, Zugriffsrechte) werden monatlich überprüft. Im Rahmen dieser Überprüfung wird zusätzlich die Login-Historie der eingesetzten Plattformen eingesehen, um unautorisierte Zugriffe zeitnah erkennen zu können.

Qualitätsprüfung der Assistenten

Vor Go-Live eines neuen Auftraggebers wird die Konfiguration des Assistenten gründlich anhand der festgelegten Standardkonfiguration geprüft; jede Funktion wird mit einem Testanruf geprüft. Im laufenden Betrieb erfolgt eine Überprüfung anlassbezogen bei auftretenden Fehlern sowie routinemäßig im Abstand von etwa zwei Monaten pro Assistent. Dabei wird stichprobenartig kontrolliert, ob die Bereinigung der Mitschriften im Qualitätsarchiv greift.

Automatische Überwachung

Der stündliche Prüflauf (Kategorie 5) überwacht Erfolgsquote und Funktionsfehler jedes Assistenten; gehäufte Fehlschläge weisen zugleich auf Störungen angebundener Dienste hin. Der tägliche Löschlauf für Verbindungsdaten, SMS und E-Mails meldet fehlgeschlagene Löschungen an den Auftragsverarbeiter. Mitteilungen der Subunternehmer zu rechtlich oder betrieblich relevanten Änderungen werden täglich automatisiert ausgewertet.

Externe Zertifizierungen der Subunternehmer

Alle eingesetzten Subunternehmer verfügen über anerkannte Sicherheitsnachweise (SOC 2 Type II bzw. ISO 27001, siehe Tabelle in Abschnitt 1.1). Über die jeweiligen Trust-/Compliance-Portale der Anbieter bzw. durch aktive Anfrage (bei Retell AI) wird jährlich überprüft, ob die Nachweise weiterhin gültig sind; das Ergebnis dieser Prüfung wird mit Datum dokumentiert. Auf dieser Grundlage wird die Eignung der eingesetzten Subunternehmer als angemessene technische und organisatorische Garantie im Sinne von Art. 28 DSGVO bewertet.

Letzte Prüfung	Ergebnis
27.06.2026	Alle fünf damaligen Subunternehmer (Twilio, Retell AI, n8n, OpenAI, Cal.com) verfügen über eine gültige SOC 2 Type II-Zertifizierung; als angemessene Garantie bewertet.
10.10.2026	Google Workspace neu aufgenommen: laut Compliance-Übersicht von Google (Stand 28.09.2026) für Gmail ISO 27001/27017/27018-zertifiziert, SOC-1/2/3-Berichte vorhanden; als angemessene Garantie bewertet. OpenAI wird nicht mehr direkt eingesetzt.

8. Maßnahmen zur Gewährleistung der Zweckbindung (Nichtverkettung)

Trennung pro Auftraggeber

Jeder Auftraggeber wird über eigene, dedizierte Objekte bzw. eindeutig zugeordnete Datensätze verarbeitet:

- Twilio: eigene, dedizierte Rufnummer pro Auftraggeber
- Retell AI: eigener, separater Assistent (Agent) pro Auftraggeber

- cal.eu: eigene Terminarten pro Auftraggeber
- n8n: ein gemeinsamer Ablauf für alle Auftraggeber; jeder Funktionsaufruf wird über die Kennung des Assistenten genau einer Konfiguration zugeordnet, und die Einträge im Qualitätsarchiv tragen dieselbe Kennung
- Google: ein gemeinsames Versandkonto; Empfänger ist jeweils die in der Konfiguration des Auftraggebers hinterlegte Adresse

Durch diese Kombination aus struktureller und logischer Trennung werden personenbezogene Daten von Anrufern unterschiedlicher Auftraggeber nicht miteinander verknüpft. Die richtige Zuordnung wird vor jedem Go-Live mit Testanrufen für jede Funktion geprüft.

Trennung von geschäftlicher und privater Nutzung

Innerhalb der eingesetzten Plattformen wird die geschäftliche Nutzung (Kundenprojekte) durch separate Workspaces, Teams bzw. Ordnerstrukturen organisatorisch von einer etwaigen privaten Nutzung getrennt.

Zweckbindung der verarbeiteten Daten

Die im Rahmen der Auftragsverarbeitung erhobenen personenbezogenen Daten (Anruferdaten) werden ausschließlich für die im VVT Absatz 2 dokumentierten Zwecke verwendet (Anrufannahme, Terminverwaltung, Benachrichtigung des Auftraggebers, Weiterleitung von Anrufen). Ergänzend werden bereinigte Mitschriften zur Qualitätssicherung und Fehleranalyse des jeweiligen Assistenten herangezogen. Diese Auswertung erfolgt ausschließlich anhand der Mitschriften des jeweils betroffenen Auftraggebers, ohne Einbeziehung oder Verknüpfung mit Daten anderer Auftraggeber, und dient ausschließlich der Verbesserung der Auftragserfüllung für diesen einen Auftraggeber. Eine darüber hinausgehende, insbesondere kundenübergreifende Nutzung (z. B. für eigene Marketingzwecke) findet nicht statt.

9. Maßnahmen zur Gewährleistung der Transparenz

Transparenz gegenüber dem Anrufer

Zu Beginn jedes Anrufs wird der Anrufer durch eine einheitliche, bei allen Assistenten verwendete Begrüßung aktiv informiert. Diese enthält: die Nennung des Auftraggebers, den Hinweis, dass es sich um einen KI-Assistenten handelt, den Hinweis, dass das Gespräch aufgezeichnet und als Mitschrift gespeichert wird, sowie die Möglichkeit, dies abzulehnen („Wenn Sie das nicht möchten, sagen Sie es einfach.“). Für jeden Auftraggeber werden zudem Datenschutzhinweise für Anrufer nach Art. 13 DSGVO bereitgestellt.

Transparenz der eigenen Verfahrensdokumentation

Die Geschäftsprozesse und Datenflüsse sind im VVT Absatz 2 dokumentiert. Die Verträge mit sämtlichen Subunternehmern liegen als Data Processing Agreements vor. Die Quellen der verarbeiteten Daten sind durch die Tätigkeitsbeschreibungen im VVT Absatz 2 durchgehend nachvollziehbar dargestellt.

Nachvollziehbarkeit von Änderungen

Änderungen an Workflows und Assistenten sind über die in n8n und Retell AI jeweils integrierte Versionshistorie nachvollziehbar (siehe Kategorie 6); wesentliche Entscheidungen werden zusätzlich in der Projektdokumentation festgehalten.

Technischer Hinweis zur Gesprächsaufzeichnung

Die Sprach-KI-Plattform verarbeitet das Gespräch technisch von Beginn an als Aufnahme; dies lässt sich nicht abschalten. Die Aufnahme wird jedoch nicht dauerhaft gespeichert (Kategorie 2). Widerspricht der Anrufer, fragt der Assistent keine Daten mehr ab; während der Geschäftszeiten

verbindet er den Anrufer direkt mit dem Auftraggeber und verlässt dabei das Gespräch. Die Rechtsgrundlagen der Verarbeitung sind in den Datenschutzhinweisen für Anrufer des jeweiligen Auftraggebers festgelegt.

10. Maßnahmen zur Gewährleistung der Betroffenenrechte (Intervenierbarkeit)

Löschung auf Anfrage Betroffener

Geht über den Auftraggeber – oder nach Weiterleitung an ihn auf dessen Weisung – eine Löschanfrage eines Anrufers ein, wird der betreffende Datensatz anhand von Datum, Uhrzeit und – soweit vorhanden – Rufnummer des Anrufs identifiziert und in den jeweils betroffenen Systemen gelöscht:

Plattform	Löschmaßnahme	Zeitliche Einschränkung
Retell AI	Löschung des Anrufeintrags (Verbindungsdaten); Mitschrift und Aufnahme werden dort nicht gespeichert	Nur innerhalb der 7-Tage-Frist; danach bereits automatisch gelöscht
n8n	Löschung des Eintrags im Qualitätsarchiv und ggf. gespeicherter Fehlerprotokolle	Nur innerhalb von 7 Tagen; danach bereits automatisch gelöscht
Twilio	Löschung des Anrufprotokolls bzw. der SMS mit der betreffenden Rufnummer	Anrufprotokolle innerhalb von 40 Tagen, SMS innerhalb von 7 Tagen
cal.eu	Löschung der Buchung bzw. des Termins, auch wenn dieser in der Vergangenheit liegt	Keine automatische Frist während aktiver Nutzung
Google	Löschung der gesendeten E-Mail im Versandkonto	Innerhalb von 30 Tagen; danach höchstens weitere 30 Tage im Papierkorb

Erfolgt die Anfrage erst nach Ablauf der jeweiligen automatischen Speicherfristen, sind die betreffenden Daten dort bereits automatisch und unwiderruflich gelöscht.

Speicherfristen und automatische Löschung

- Qualitätsarchiv (n8n): 7 Tage; täglicher Löschlauf.
- Fehlerprotokolle (n8n): höchstens 7 Tage; automatische Löschung durch n8n. Erfolgreiche Abläufe werden nicht gespeichert.
- Verbindungsdaten bei Retell AI: 7 Tage.
- Anrufprotokolle der Rufnummern des Telefonassistenten (Twilio): 40 Tage; täglicher Löschlauf.
- SMS vom Absender „Kalendria“ (Twilio): 7 Tage; täglicher Löschlauf. Die Aufbewahrung von Nachrichten im Twilio-Konto ist auf 7 Tage begrenzt, Sicherungskopien sind abgeschaltet.
- Gesendete E-Mails mit Anruferdaten (Google): nach 30 Tagen in den Papierkorb (täglicher Löschlauf), endgültige Löschung nach höchstens weiteren 30 Tagen.
- Der tägliche Löschlauf erfasst nur Daten, die eindeutig dem Telefonassistenten zugeordnet sind (Rufnummern des Telefonassistenten, Absender „Kalendria“, bekannte Betreffzeilen der Benachrichtigungen), und meldet fehlgeschlagene Löschungen an den Auftragsverarbeiter.

Kontaktweg für Betroffenenanfragen

Jedem Auftraggeber wird eine Kontakt-E-Mail-Adresse zur Verfügung gestellt, die dieser bei Bedarf an Anrufer weitergeben kann, die eine Löschung oder Auskunft zu ihren Daten wünschen. Gehen Anfragen

direkt beim Auftragsverarbeiter ein, leitet er sie unverzüglich an den Auftraggeber weiter und setzt sie nach dessen Weisung um (Art. 28 Abs. 3 lit. e DSGVO).

11. Schlussbemerkung

Dieses Dokument wird bei wesentlichen Änderungen der eingesetzten Systeme, Subunternehmer oder Verarbeitungsprozesse aktualisiert. Es wird im Rahmen der jährlichen Überprüfung (siehe Kategorie 7) auf Aktualität geprüft und bei Bedarf angepasst.