

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 Abs. 1 DSGVO

Auftragsverarbeiter	Felix Oskar Griebeler
Kontakt	felix@griebeler.eu
Geltungsbereich	Bereitstellung eines KI-gestützten telefonischen Rezeptionisten für Betriebe des SHK-Handwerks (Sanitär, Heizung, Klima) auf Basis der Plattformen Twilio, Retell AI, n8n, OpenAI und cal.eu (Cal.com)
Stand / Version	07.07.2026 – Version 1.1
Referenzdokument	Verzeichnis von Verarbeitungstätigkeiten (VVT) – Auftragsverarbeiter, Art. 30 Abs. 2 DSGVO

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 als Referenzdokument im Verzeichnis von Verarbeitungstätigkeiten (VVT) sowie in 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.	Telefonie-Infrastruktur, SMS-Versand	SOC 2 Type II, ISO 27001/17/18, PCI DSS
Retell AI, Inc.	KI-Sprachagent-Plattform	SOC 2 Type II (auf Anfrage)
n8n GmbH	Workflow-Orchestrierung	SOC 2 Type II
OpenAI Ireland Ltd.	Sprachmodell (Dialog, Textgenerierung)	SOC 2 Type II, ISO 27001/17/18/701
Cal.com, Inc. (cal.eu)	Terminverwaltung (EU-Hosting)	SOC 2 Type II, ISO 27001

Hinsichtlich Azure (Transkription) und ElevenLabs (Sprachsynthese) handelt es sich um 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.

2. Pseudonymisierung personenbezogener Daten

Automatisierte PII-Redaction bei Retell AI

Nach Abschluss eines Anrufs werden in Retell AI automatisiert personenbezogene Daten im Gesprächstranskript und in der Audioaufzeichnung erkannt und entfernt (Redaction). 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

Technische Umsetzung

Im Transkript werden erkannte personenbezogene Daten durch standardisierte Platzhalter ersetzt (z. B. „[person name]“, „[email]“). In der Audioaufzeichnung werden die entsprechenden Sprachpassagen akustisch durch einen Piepton überdeckt. Die Bereinigung erfolgt unmittelbar nach Gesprächsende und vor der dauerhafteren Speicherung.

Einordnung der übrigen Subunternehmer

Twilio, n8n, OpenAI und cal.eu verarbeiten im Rahmen der jeweiligen Verarbeitungstätigkeit bewusst nicht-pseudonymisierte Daten, da dies für den jeweiligen Zweck (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, OpenAI, cal.eu) 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 (n8n zu cal.eu, OpenAI und Twilio) erfolgen ausschließlich über verschlüsselte HTTPS/TLS-Verbindungen.
- Die Webhook-Kommunikation zwischen Retell AI und n8n ist zusätzlich durch eine Header-Authentifizierung mittels eines geheimen Token abgesichert, sodass ausschließlich autorisierte Anfragen den Workflow auslösen können.

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, OpenAI und cal.eu.
- 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 6) wird zusätzlich die Login-Historie der eingesetzten Plattformen eingesehen, um unautorisierte Zugriffe zeitnah erkennen zu können.

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 Drittdienstes (cal.eu, OpenAI oder Twilio), während n8n selbst funktionsfähig ist: n8n antwortet dem Retell-Agenten aktiv mit einer Fehlermeldung (z. B. dass eine Terminbuchung, -verschiebung oder -stornierung aktuell nicht möglich ist). Der Agent erhält diese Information unmittelbar und kann sie im laufenden Gespräch kommunizieren.
2. Ausfall von n8n selbst (keine Antwort): Die Webhook-Anfrage wartet bis zu 2 Minuten auf eine Rückmeldung (Timeout). Während dieser Wartezeit führt die KI-gestützte Gesprächsführung das Gespräch aktiv und durchgehend weiter (z. B. durch Überbrückung, Rückfragen oder Fortsetzung ohne die betroffenen Daten) – das Gespräch wird nicht unterbrochen. Bleibt die Antwort weiterhin aus, werden bis zu zwei weitere Anfrageversuche unternommen.

In beiden Fällen wird der Anrufer nicht ohne Reaktion gelassen – entweder durch eine aktive Fehlerinformation aus n8n oder durch die durchgehende, aktive Gesprächsführung während der Wartezeit.

Sicherung und Testumgebung für Workflow- und Agent-Konfiguration

Die n8n-Workflow-Konfiguration (als JSON-Export) sowie die Retell-Agent-Konfiguration werden als separate, laufend aktualisierte Kopien gesichert. Diese Kopien dienen zugleich als Testumgebung, in der Fehlerbehebungen und Anpassungen vorgenommen und geprüft werden können, ohne das produktiv laufende System zu beeinträchtigen.

Umgang mit länger andauernden Plattformaussfällen

Für den Telefon-Agenten ist in Retell AI ein automatisiertes Alerting eingerichtet, das zwei konkrete, ausschließlich auf aggregierten Metrikwerten basierende Schwellenwerte überwacht: die Erfolgsquote der Gespräche (Call Success Rate, Schwellwert unter 70 % im 24-Stunden-Fenster) sowie die Anzahl

fehlgeschlagener technischer Funktionsaufrufe (Number of Custom Function Failures, Schwellwert über 1 im 1-Stunden-Fenster). Bei Überschreitung eines Schwellwerts löst Retell AI automatisch einen Webhook an eine dedizierte n8n-Automatisierung aus. Diese leitet die dem Agenten zugeordnete Twilio-Rufnummer automatisiert auf die Betriebsnummer des Auftraggebers um – technisch durch Anpassung der Sprachkonfiguration der Rufnummer bei Twilio, nicht durch Deaktivierung des Agenten in Retell AI selbst – und benachrichtigt sowohl den Auftragsverarbeiter als auch den Auftraggeber automatisiert per SMS. Die Umleitung bleibt bestehen, bis sie nach Behebung der Störung durch den Auftragsverarbeiter manuell zurückgesetzt wird. Das konkrete Vorgehen für Ausfallszenarien, die von diesem automatisierten Alerting nicht erfasst werden, wird ergänzend individuell mit jedem Auftraggeber vor Go-Live abgestimmt.

Dokumentiertes Restrisiko

Ein vollständiger Ausfall der Retell-AI-Plattform selbst (einschließlich deren Monitoring-Funktion) liegt außerhalb der eigenen Einflussmöglichkeiten und wird durch die Verfügbarkeitszusagen des Anbieters 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.

Staging-Umgebung pro Kunde

Für jeden Auftraggeber wird eine separate, mit dem jeweiligen Live-System identische Kopie des Agenten und Workflows als Testumgebung vorgehalten. Sowohl technische Änderungen als auch inhaltliche Qualitätsverbesserungen werden zunächst dort getestet, bevor sie in das produktive System übernommen werden.

Automatisierte Anrufumleitung bei Systemausfall

Wird eine Störung über das in Kategorie 5 beschriebene automatisierte Alerting festgestellt, erfolgt die Umleitung der Anrufe auf die Betriebsnummer automatisiert durch den Auftragsverarbeiter; eine gesonderte Handlung des Auftraggebers ist hierfür nicht erforderlich. Vor Go-Live wird mit jedem Auftraggeber ergänzend abgestimmt, wie im Falle einer Störung zu verfahren ist, die von diesem automatisierten Alerting nicht erfasst wird.

Dokumentiertes Restrisiko

Zwischen dem Eintritt einer Störung und der automatisierten Umleitung verbleibt eine durch die Prüfintervalle des Alertings bedingte Zeitspanne (bis zu 30 Minuten bzw. 1 Stunde, je nach Metrik), innerhalb derer eingehende Anrufe weiterhin unmittelbar beim Agenten verarbeitet werden. Fällt zudem die eingesetzte Automatisierungsplattform (n8n) oder Twilio selbst aus, kann die automatisierte Umleitung nicht ausgeführt werden; in einem solchen Fall verbleiben in Twilio lediglich Metadaten des eingehenden Anrufs (insbesondere die anrufende Telefonnummer), jedoch ohne Zuordnung zu Name oder Anliegen. Eine Weitergabe dieser Telefonnummer an den Auftraggeber ist keine reguläre, angebotene Maßnahme, sondern ausschließlich auf ausdrückliche, im Einzelfall begründete Anfrage hin möglich.

Keine eigene Anrufaufzeichnung

Eine zusätzliche eigene Aufzeichnung abgeschlossener Anrufe außerhalb der eingesetzten Plattformen wird nicht geführt.

Verhältnismäßige Reaktion auf Plattform-Störungen

Bei einem geringfügigen, isolierten und nicht öffentlich kommunizierten Vorfall bei einer eingesetzten Plattform wird der betroffene Agent 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 Agent hingegen offline genommen; dies gilt einheitlich für alle eingesetzten Plattformen.

Offline-Nahme bei Qualitätsproblemen

Unabhängig von der technischen Verfügbarkeit der eingesetzten Plattformen wird ein Agent auch dann offline genommen, überarbeitet und in der Staging-Umgebung getestet, 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 Agenten 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.

Agent-Qualitätsprüfung

Vor Go-Live eines neuen Auftraggebers wird die Agent-Konfiguration gründlich anhand der festgelegten Standardkonfigurationen geprüft. Im laufenden Betrieb erfolgt eine Überprüfung anlassbezogen bei auftretenden Fehlern sowie routinemäßig im Abstand von etwa zwei Monaten pro Agent.

Live-Monitoring

Über das in Retell AI integrierte Live-Monitoring wird die Agent-Qualität im laufenden Betrieb überwacht (Zielerreichung, Erfolgsquote technischer Funktionsaufrufe). Dieselbe Konfiguration dient zugleich als indirekter Indikator für zugrunde liegende Plattformaussfälle (siehe Kategorie 5), da gehäufte Fehlschläge häufig auf eine Störung bei einem der angebundenen Drittdienste hinweisen.

Externe Zertifizierungen der Subunternehmer

Alle eingesetzten Subunternehmer (Twilio, Retell AI, n8n, OpenAI, cal.eu/Cal.com) verfügen über eine SOC 2 Type II-Zertifizierung (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 Zertifizierungen 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 Subunternehmer verfügen über eine gültige SOC 2 Type II-Zertifizierung; als angemessene Garantie bewertet.
------------	--

8. Maßnahmen zur Gewährleistung der Zweckbindung (Nichtverkettung)

Strukturelle Mandantentrennung pro Auftraggeber

Sämtliche eingesetzten Plattformen sind so konfiguriert, dass jeder Auftraggeber über vollständig separate, dedizierte Objekte verarbeitet wird:

- Twilio: eigene, dedizierte Telefonnummer pro Auftraggeber
- Retell AI: eigener, separater Agent pro Auftraggeber
- n8n: eigener, separater Workflow pro Auftraggeber
- cal.eu: eigener Event-Type pro Auftraggeber
- OpenAI: eigener API-Key pro Auftraggeber

Durch diese strukturelle (nicht nur logische) Trennung wird ausgeschlossen, dass personenbezogene Daten von Anrufern unterschiedlicher Auftraggeber miteinander verknüpft werden oder sich versehentlich vermischen.

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 Verzeichnis von Verarbeitungstätigkeiten dokumentierten Zwecke verwendet (Anrufannahme, Terminverwaltung, Benachrichtigung des Auftraggebers). Ergänzend werden bereits PII-redactete Gesprächstranskripte zur Qualitätssicherung und Fehleranalyse des jeweiligen Agenten herangezogen, sofern dieser inhaltliche Mängel aufweist. Diese Auswertung erfolgt ausschließlich anhand der Transkripte des jeweils betroffenen Auftraggebers, ohne Einbeziehung oder Verknüpfung mit Daten anderer Auftraggeber, und dient ausschließlich der Verbesserung der Auftragserfüllung für diesen einen Auftraggeber. Eine darüberhinausgehende, 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 Kunden-Agenten verwendete Begrüßungsnachricht aktiv informiert. Diese enthält mindestens: die Nennung des Auftraggebers, den Hinweis, dass es sich um einen digitalen KI-Assistenten handelt, sowie den Hinweis, dass das Gespräch zu Qualitätssicherungszwecken aufgezeichnet wird.

Transparenz der eigenen Verfahrensdokumentation

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

Nachvollziehbarkeit von Änderungen

Eine gesonderte, manuell gepflegte Änderungsdokumentation wird aktuell nicht geführt. Änderungen an Workflows und Agent-Konfigurationen sind jedoch über die in n8n und Retell AI jeweils integrierte Versionshistorie nachvollziehbar (siehe Kategorie 6).

Technischer Hinweis zur Gesprächsaufzeichnung

Die Gesprächsaufzeichnung beginnt automatisch mit Gesprächsstart und kann durch den Agenten technisch nicht gestoppt oder unterbrochen werden. Der Anrufer wird hierüber zu Beginn des Gesprächs transparent informiert (siehe oben). Die rechtliche Grundlage der Verarbeitung (Einwilligung, Vertragserfüllung oder berechtigtes Interesse) wird gesondert im Rahmen der Datenschutzerklärung des jeweiligen Auftraggebers festgelegt.

10. Maßnahmen zur Gewährleistung der Betroffenenrechte (Intervenierbarkeit)

Löschung auf Anfrage Betroffener

Geht – direkt oder über den Auftraggeber – eine Löschanfrage eines Anrufers ein, wird der betreffende Datensatz anhand von Datum und Uhrzeit des Anrufs identifiziert und in den jeweils betroffenen Systemen manuell gelöscht:

Plattform	Löschmaßnahme	Zeitliche Einschränkung
Retell AI	Löschung von Transkript und Audioaufzeichnung über die Anruf-Historie	Nur innerhalb der 7-Tage-Speicherfrist; danach bereits automatisch gelöscht
OpenAI	Löschung der API-Response-Daten	Nur innerhalb der 30-Tage-Speicherfrist relevant
Twilio	Löschung des Call-Logs bzw. der SMS-Inhalte mit der betreffenden Telefonnummer	Innerhalb der geltenden 13-Monats-Frist
cal.eu	Löschung der Buchung/des Termins, auch wenn dieser in der Vergangenheit liegt	Keine automatische zeitliche Frist während aktiver Nutzung
n8n	Keine Maßnahme erforderlich	Es findet keine Speicherung statt

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

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. Anfragen können somit sowohl über den Auftraggeber als auch direkt durch den Anrufer eingehen.

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.