Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 8. November 2026

Für die Telefonanlage SONOPOLAR: Cloud-Dienst sowie Push-Vermittler, Support-Aufschaltung und Tarif Managed bei On-Premise-Anlagen.

Parteien

Verantwortlicher (Auftraggeber):
Firma, Rechtsform: _____
Anschrift: _____
vertreten durch: _____
im Folgenden „Kunde“

Auftragsverarbeiter (Auftragnehmer):
KREATIKA, Maximilian A. Grimm, Kuglerstraße 2, 90449 Nürnberg, Deutschland
E-Mail: grimm@kreatika.de, USt-IdNr. DE249433890
im Folgenden „KREATIKA“

Dieser Vertrag ist auf sonopolar.com/av-vertrag.html veröffentlicht. Er gilt mit der Bestellung des Kunden als geschlossen, ohne dass es einer Unterschrift bedarf. Wünscht der Kunde eine unterschriebene Fassung, füllt er die Felder oben und am Ende aus und sendet das Dokument an grimm@kreatika.de; KREATIKA sendet es gegengezeichnet zurück.

§ 1 Gegenstand und Dauer

(1) KREATIKA verarbeitet im Auftrag des Kunden personenbezogene Daten im Rahmen der folgenden Leistungen, soweit der Kunde sie bezieht (Hauptvertrag):

- **Cloud-Dienst:** KREATIKA betreibt für den Kunden die Telefonanlage SONOPOLAR auf eigenen Servern nach den AGB für den Cloud-Dienst.
- **Push-Vermittler:** Eine On-Premise-Anlage des Kunden sendet Benachrichtigungen an die Apps über den Vermittler von KREATIKA (push.sonopolar.com).
- **Support-Aufschaltung:** KREATIKA greift mit Freigabe des Kunden über einen Tunnel auf die Verwaltung seiner On-Premise-Anlage zu.
- **Tarif Managed:** KREATIKA betreut die On-Premise-Anlage des Kunden laufend; der Support-Zugang ist dabei dauerhaft freigegeben.

Gegenstand, Art und Zweck, Datenarten und Betroffene stehen in Anlage 1.

(2) Dieser Vertrag gilt, solange der Hauptvertrag läuft, und darüber hinaus, solange KREATIKA noch Daten des Kunden verarbeitet (§ 10).

(3) Betreibt der Kunde SONOPOLAR On-Premise ohne die Leistungen nach Absatz 1, verarbeitet KREATIKA keine Daten seiner Anlage, und dieser Vertrag findet keine Anwendung. Der tägliche Heimruf einer On-Premise-Anlage (Lizenzbedingungen § 8) überträgt keine Daten von Nutzern oder Gesprächen; KREATIKA verarbeitet ihn als eigene Vertragsdaten.

§ 2 Weisungen

(1) KREATIKA verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in Drittländer, es sei denn, KREATIKA ist nach Unionsrecht oder deutschem Recht zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In diesem Fall teilt KREATIKA dem Kunden die rechtliche Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Der Hauptvertrag und die Einstellungen, die der Kunde in der Verwaltung der Anlage vornimmt (etwa Aufzeichnung, Weiterleitungen, Mailversand von Sprachnachrichten, Webhooks, Freigabe oder Pause der Support-Aufschaltung), gelten als Weisung.

(3) Weitere Weisungen erteilt der Kunde in Textform an grimm@kreatika.de. Weisungsberechtigt beim Kunden sind die gesetzlichen Vertreter, die bei der Bestellung genannte Ansprechperson und die Personen mit Rolle Admin in der Anlage, soweit der Kunde in Textform nichts anderes bestimmt. Weisungsempfänger bei KREATIKA ist Maximilian A. Grimm.

(4) Hält KREATIKA eine Weisung für rechtswidrig, weist KREATIKA den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO) und darf die Ausführung aussetzen, bis der Kunde sie bestätigt oder ändert.

§ 3 Vertraulichkeit und Fernmeldegeheimnis

(1) KREATIKA setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) KREATIKA wirkt am Telekommunikationsdienst des SIP-Anbieters des Kunden mit und wahrt das Fernmeldegeheimnis nach § 3 TDDDG. Die eingesetzten Personen werden darauf verpflichtet. Von Inhalten und näheren Umständen der Gespräche nimmt KREATIKA nur Kenntnis, soweit es für Betrieb, Störungsbeseitigung oder Schutz der Anlage erforderlich ist.

(3) Die Software unterstützt das technisch: Meldet sich der Betreiber, der Support oder ein Admin in der Sitzung einer anderen Nebenstelle an, sind dort Gesprächsinhalte und Verbindungsdaten gesperrt (Chat, Mailbox, Anrufliste, Aufzeichnungen, Berichte, Live-Ansicht, Telefon). Über die Support-Aufschaltung sind Verbindungsdaten nicht abrufbar. Jede solche Sitzung steht im Ereignisprotokoll des Kunden.

§ 4 Technische und organisatorische Maßnahmen

(1) KREATIKA trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 3 beschrieben sind. Die jeweils aktuelle Fassung steht auf sonopolar.com/toms.html.

(2) KREATIKA darf die Maßnahmen an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt. Wesentliche Änderungen teilt KREATIKA dem Kunden in Textform mit.

§ 5 Unterauftragsverarbeiter

(1) Der Kunde genehmigt die in Anlage 4 genannten Unterauftragsverarbeiter. Die jeweils aktuelle Liste steht auf sonopolar.com/unterauftragsverarbeiter.html.

(2) KREATIKA informiert den Kunden mindestens 30 Tage vorher in Textform über jede beabsichtigte Änderung (Hinzuziehung oder Ersetzung). Der Kunde kann innerhalb von 14 Tagen nach Zugang der Mitteilung aus wichtigem datenschutzrechtlichem Grund widersprechen. Einigen sich die Parteien nicht, kann der Kunde den Hauptvertrag zum Zeitpunkt der Änderung kündigen. In dringenden Fällen, etwa beim Ausfall eines Unterauftragsverarbeiters, darf KREATIKA mit kürzerer Frist wechseln; das Recht zum Widerspruch und zur Kündigung bleibt.

(3) KREATIKA legt jedem Unterauftragsverarbeiter dieselben Datenschutzpflichten auf, die dieser Vertrag enthält (Art. 28 Abs. 4 DSGVO), soweit dieser nicht nur standardisierte Bedingungen anbietet, die ein gleichwertiges Schutzniveau sichern.

(4) Keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Leistungen, die der Kunde selbst bei Dritten bezieht, auch wenn die Anlage technisch mit ihnen verbunden ist. Das sind insbesondere:

- **der SIP-Anbieter des Kunden** (zum Beispiel easybell): Der Kunde schließt den Vertrag über Anschluss und Rufnummern selbst. Die Anlage meldet sich mit den Zugangsdaten des Kunden beim Anbieter an und stellt dort Gespräche zu. Der Anbieter erbringt einen eigenen Telekommunikationsdienst gegenüber dem Kunden.
- **Microsoft 365 / Entra ID und Google**, soweit der Kunde oder seine Nutzer die Anlage damit verbinden (Anmeldung mit Microsoft, Abgleich von Nutzern und Gruppen, Import von Kontakten). Die Anlage liest dort mit der Berechtigung, die der Kunde oder der Nutzer erteilt; in Microsoft ändert sie nichts. Das Verhältnis zu Microsoft oder Google besteht zwischen dem Kunden und dem jeweiligen Anbieter.
- **Ziele von Webhooks und Programmierschnittstellen**, die der Kunde selbst einträgt.
- **Dienste des Betriebssystems der Endgeräte**, etwa Siri und CarPlay auf dem iPhone, soweit der Nutzer sie für die App einschaltet.

§ 6 Unterstützung des Kunden

(1) KREATIKA unterstützt den Kunden mit geeigneten Maßnahmen bei der Erfüllung der Rechte der Betroffenen nach Art. 12 bis 22 DSGVO. Vieles kann der Kunde selbst in der Verwaltung erledigen: Nutzer, Kontakte, Aufzeichnungen und Sprachnachrichten löschen, Gesprächsdaten als CSV ausgeben, Geräte abmelden. Was darüber hinausgeht, erledigt KREATIKA auf Anfrage. Wendet sich ein Betroffener direkt an KREATIKA, leitet KREATIKA die Anfrage unverzüglich an den Kunden weiter.

(2) KREATIKA unterstützt den Kunden bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Meldungen von Datenschutzverletzungen und bei einer Datenschutz-Folgenabschätzung, etwa durch die Vorlage mit der technischen Beschreibung der Gesprächsaufzeichnung.

(3) Für Unterstützung, die über das hinausgeht, was die Anlage selbst bereitstellt, kann KREATIKA eine Vergütung nach Aufwand verlangen: 107 Euro je Stunde zuzüglich Umsatzsteuer, abgerechnet je angefangene Viertelstunde. Das gilt nicht, wenn die Unterstützung durch einen Verstoß von KREATIKA nötig wurde.

§ 7 Meldung von Verletzungen

KREATIKA meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 24 Stunden nachdem KREATIKA davon Kenntnis erlangt hat, in Textform an die hinterlegte Adresse des Kunden. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben reicht KREATIKA nach, sobald sie vorliegen. Die Meldung an die Aufsichtsbehörde und an Betroffene bleibt Sache des Kunden.

§ 8 Nachweise und Kontrollen

(1) KREATIKA stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO nötig sind.

(2) Der Kunde oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer, der kein Wettbewerber von KREATIKA ist, darf nach Anmeldung mit 14 Tagen Vorlauf zu den üblichen Geschäftszeiten prüfen, höchstens einmal im Jahr, es sei denn, es besteht ein konkreter Anlass. Die Räume des Rechenzentrums gehören dem Unterauftragsverarbeiter; dort genügen dessen Zertifikate und Prüfberichte. Den Aufwand für Prüfungen trägt jede Seite selbst; Vor-Ort-Prüfungen ohne Anlass, die länger als einen Arbeitstag dauern, vergütet der Kunde nach § 6 Abs. 3.

§ 9 Ort der Verarbeitung

Die Anlage, ihre Datenbank und ihre Sicherungen liegen in Rechenzentren der Hetzner Online GmbH in Deutschland. Eine Verarbeitung außerhalb der EU und des EWR findet nur in dem Umfang statt, der in Anlage 4 für die Push-Dienste beschrieben ist.

§ 10 Löschung und Rückgabe

(1) Nach Ende des Hauptvertrags und eines Abrufzeitraums von 30 Tagen löscht KREATIKA den Mandanten des Kunden. Das Löschen des Mandanten entfernt in der Datenbank alle zugehörigen Datensätze (Nebenstellen, Gesprächsdaten, Kontakte, Firmentelefonbuch, Chats, Aufzeichnungen, Sprachnachrichten, Geräte und Weiteres) und vom Datenträger die Dateien des Mandanten (Ansagen, Sprachnachrichten, Aufzeichnungen, Fotos, Logos und Schriften).

(2) Auf Wunsch übergibt KREATIKA dem Kunden vor der Löschung seine Daten als ZIP-Archiv zum Herunterladen: Nebenstellen, Rufnummern, Rufgruppen, Kontakte und Firmentelefonbuch, Verbindungsdaten, Chatnachrichten und Ereignisprotokoll als CSV-Dateien (UTF-8), Aufzeichnungen, Sprachnachrichten und Ansagen als WAV-Dateien mit einer Liste der Zuordnung, auf Wunsch zusätzlich ein Auszug der Datenbank des Mandanten im Format von PostgreSQL. Kennwörter und Schlüssel werden nicht übergeben.

(3) In den Datensicherungen bleiben Daten bis zum Ablauf ihrer Aufbewahrung erhalten (Anlage 2). Sie werden nicht mehr verwendet und danach mit dem Sicherungsstand gelöscht.

(4) Bei den On-Premise-Leistungen nach § 1 Abs. 1 speichert KREATIKA keine Daten der Anlage dauerhaft; Absatz 1 bis 3 gelten für die Protokolle nach Anlage 2 entsprechend.

§ 11 Haftung

Für die Haftung im Außenverhältnis gilt Art. 82 DSGVO. Im Innenverhältnis gilt die Haftungsregelung des Hauptvertrags; sie begrenzt nicht die Haftung für Verstöße von KREATIKA gegen diesen Vertrag oder die DSGVO, soweit Art. 82 Abs. 4 und 5 DSGVO eine Verteilung nach dem Anteil der Verantwortung vorsehen.

§ 12 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag vor, soweit es um den Schutz personenbezogener Daten geht.

(2) Änderungen bedürfen der Textform. Für Änderungen dieses Vertrags durch KREATIKA gilt § 13 der AGB für den Cloud-Dienst entsprechend; Änderungen der Anlagen 3 und 4 richten sich nach § 4 Abs. 2 und § 5 Abs. 2.

(3) Ist eine Bestimmung unwirksam, bleibt der Rest wirksam.

(4) Es gilt deutsches Recht. Gerichtsstand ist Nürnberg, soweit der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Ort, Datum, Unterschrift Kunde: _____

Nürnberg, Datum, Unterschrift KREATIKA: _____

Anlage 1: Gegenstand, Art und Zweck, Datenarten, Betroffene

Gegenstand und Zweck

Cloud-Dienst: Bereitstellung und Betrieb einer Telefonanlage für den Kunden: Vermittlung interner, eingehender und ausgehender Gespräche über den SIP-Anschluss des Kunden, Portal mit Telefon im Browser, App für iPhone und Android, Tischtelefone, Anrufbeantworter, Warteschleifen, Ansagemenüs, Konferenzen, Chat, Präsenz, Kontakte und Firmentelefonbuch, Gesprächsaufzeichnung nach Einstellung des Kunden, Berichte, Datensicherung, Wartung und Fehlerbehebung.

Push-Vermittler (On-Premise): Weiterleiten der Weckmeldungen der Anlage des Kunden an den Apple Push Notification Service und Firebase Cloud Messaging, weil die Schlüssel dafür bei KREATIKA liegen.

Support-Aufschaltung und Tarif Managed (On-Premise): Fehlersuche, Einrichtung, Updates und Betreuung über die Verwaltung der Anlage des Kunden.

Art der Verarbeitung

Erheben, Speichern, Vermitteln, Anzeigen, Abspielen, Übermitteln an die vom Kunden eingerichteten Ziele (SIP-Anbieter, Mail, Webhooks), Weiterleiten von Weckmeldungen, Einsehen und Ändern über die Verwaltung, Sichern, Löschen.

Datenarten

Datenart	Inhalt nach Datenmodell der Anlage
Stammdaten der Nutzer	Nebenstelle, Anzeigename, Vor- und Nachname, E-Mail, Mobilnummer, Foto (hochgeladen oder aus Microsoft), Rolle, Abteilung, Kennung aus Microsoft Entra ID
Zugangsdaten	SIP-Kennwort nur als Hash (HA1), Portal-Kennwort und Mailbox-PIN als scrypt-Hash, Schlüssel der Zwei-Faktor-Anmeldung verschlüsselt, Wiederherstellungscodes als SHA-256, Sitzungen der App als Hash, Zugangstoken für Microsoft- oder Google-Konten der Nutzer
Rufnummern und Einstellungen	Rufnummern des Kunden, Weiterleitungen, Rufgruppen, Geschäftszeiten, Sperrlisten, Ansagen
Verbindungsdaten (CDR)	Richtung, Rufnummer des Anrufers und des Ziels, Beginn, Annahme, Ende, Dauer, Grund der Beendigung
Mailbox-Nachrichten	Audiodatei, Nummer und Name des Anrufers, Dauer, Zeitpunkt, gehört ja/nein
Gesprächsaufzeichnungen	Audiodatei (WAV) des Gesprächs, Nebenstelle, Gesprächskennung, Beginn und Ende
Chat	Nachrichtentext, Absender, Raum, Zeitpunkt
Kontakte	persönliche Kontakte je Nebenstelle (Name, Firma, Rufnummern, E-Mail), auch importiert aus Microsoft 365 oder Google
Firmentelefonbuch	Name, Firma, Abteilung, Funktion, Rufnummern, E-Mail, Notizen
Präsenz	Status (verfügbar, Nicht stören, Statustext), Anmeldezustand der Telefone, laufende Gespräche
Gerätedaten	Tischtelefone: MAC-Adresse, Modell, letzte IP-Adresse, Kennung der Software; Apps und Browser: Gerätename, Plattform, App-Version, Push-Adresse und Schlüssel des Abos, Browserkennung, Zeitpunkt der letzten Zustellung

Datenart	Inhalt nach Datenmodell der Anlage
Protokolle	Ereignisprotokoll der Verwaltung (wer hat wann was geändert, wer hat welche fremde Aufzeichnung angehört, Anmeldungen als andere Nebenstelle, Seiten und Aktionen des Supports), Fehlanmeldungen mit Quelladresse
Push-Vermittler	Installationskennung, Push-Adresse des Geräts (Token), verschlüsselte Meldung; Name und Nummer des Anrufers nur im Klartext, wenn der Kunde das eingeschaltet hat

Kategorien betroffener Personen

- Beschäftigte und sonstige Nutzer des Kunden mit Nebenstelle
- Anrufer und Angerufene außerhalb des Kunden (Kunden, Lieferanten, Interessenten des Kunden)
- Personen im Firmentelefonbuch und in den Kontakten der Nutzer

Besondere Kategorien nach Art. 9 DSGVO werden nicht gezielt verarbeitet. Sie können aber im Inhalt von Gesprächsaufzeichnungen, Sprachnachrichten und Chats vorkommen, ohne dass KREATIKA davon Kenntnis nimmt.

Anlage 2: Aufbewahrung

Daten	Aufbewahrung in der Cloud-Anlage
Gesprächsaufzeichnungen	90 Tage, dann tägliches automatisches Löschen von Datei und Eintrag; früher, wenn der Kunde sie löscht
Verbindungsdaten (CDR)	365 Tage, dann tägliches automatisches Löschen
Sprachnachrichten	90 Tage, dann tägliches automatisches Löschen mit Datei
Chatnachrichten	365 Tage, dann tägliches automatisches Löschen
Ereignisprotokoll	730 Tage, dann tägliches automatisches Löschen
Kontakte, Firmentelefonbuch, Nebenstellen, Einstellungen	bis zum Löschen durch den Kunden oder bis zum Löschen des Mandanten
Daten einer gelöschten Nebenstelle	sofort mit der Nebenstelle, einschließlich ihrer Aufzeichnungs-, Sprachnachrichten- und Fotodateien
Sicherung auf dem Server	14 Tage, ohne Aufzeichnungen und Sprachnachrichten
Sicherung des ganzen Systems	7 tägliche, 4 wöchentliche und 6 monatliche Stände, also höchstens rund sechs Monate; die Kopie außer Haus folgt denselben Ständen
Push-Vermittler	keine Speicherung; nur ein Zähler je Installation und Minute im Arbeitsspeicher
Support-Aufschaltung	Protokoll der Seiten und Aktionen beim Kunden nach dessen Frist für das Ereignisprotokoll; Protokoll der Aufschaltung bei KREATIKA 730 Tage

Die Fristen gelten für die ganze Cloud-Anlage, nicht je Mandant. Kürzere Fristen für einen Mandanten vereinbart der Kunde mit KREATIKA in Textform.

Anlage 3: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Beschrieben ist, was die Software tut und wie KREATIKA sie betreibt. Stand: 8. November 2026.

Vertraulichkeit

Zutritt (Rechenzentrum): Server und Sicherungen stehen in Rechenzentren der Hetzner Online GmbH in Deutschland. Zutrittskontrolle nach den Maßnahmen von Hetzner (elektronische Zutrittskontrolle, Videoüberwachung, Sicherheitspersonal, Zertifizierung nach ISO/IEC 27001).

Zugang zu den Systemen:

- Die Anlage läuft in einem eigenen Container auf einem Server von KREATIKA. Anmeldung am Server nur über SSH mit Schlüssel; die Anmeldung mit Kennwort ist abgeschaltet.
- Die Verwaltung der Cloud-Anlage für den Betreiber ist nur aus dem internen Netz von KREATIKA (verschlüsseltes VPN) erreichbar.
- Steuerkanal zwischen Anlage und Vermittlungssoftware (Event Socket) lauscht nur lokal, Kennwort aus der Umgebung, nicht in der Konfigurationsdatei. Die interne Schnittstelle der Anlage bindet nur lokal und verlangt einen Schlüssel.
- Von außen erreichbar sind nur HTTPS (Portal, Verwaltung der Kunden, verschlüsselter WebSocket für Browser und App), SIP über TLS (Port 5061) und Sprache (RTP). Unverschlüsseltes SIP (Port 5060) ist von außen gesperrt.
- Keine Demo-Nutzer, keine Beispielkonfiguration: Nebenstellen, Dialplan und Anbieter kommen ausschließlich aus der Datenbank.

Zugang zur Anlage (Nutzer):

- SIP-Anmeldung nur mit Kennwort; Anrufe ohne Anmeldung werden abgewiesen (407), unbekannte Nutzer ebenso (403).
- Sperre nach Fehlanmeldungen an SIP in zwei Stufen: Die Anlage sperrt eine Quelladresse nach 10 Fehlversuchen in 10 Minuten für 60 Minuten; zusätzlich sperrt fail2ban sie nach 10 Fehlversuchen in 10 Minuten für eine Stunde auf allen Ports, bei Wiederholung jeweils doppelt so lange, höchstens eine Woche.
- Portal: Sperre nach fünf Fehlversuchen je Nebenstelle innerhalb von zehn Minuten; Kennwort und Code der Zwei-Faktor-Anmeldung zählen gemeinsam.
- Zwei-Faktor-Anmeldung (TOTP) je Nutzer, vom Kunden für alle verpflichtend schaltbar; Einmalcodes gelten nur einmal. Bei Anmeldung mit Microsoft gilt die Mehrfaktor-Anmeldung des Kunden in Entra ID.
- Kennwörter nur als Hash: SIP als HA1, Portal-Kennwort und Mailbox-PIN mit scrypt und Salz. Schlüssel der Zwei-Faktor-Anmeldung mit AES-256-GCM verschlüsselt, Wiederherstellungscodes als SHA-256.
- Apps melden sich mit einem Geräteschlüssel an, nicht mit dem Kennwort. Der Kunde kann jedes Gerät aus der Ferne abmelden.

Zugriff (Berechtigungen):

- Rollen Nutzer und Admin je Mandant. Aufzeichnungen aller Nebenstellen und Berichte nur für Admins; jeder Nutzer sieht seine eigenen. Hört ein Admin eine fremde Aufzeichnung an, steht das im Ereignisprotokoll.

- Meldet sich ein Admin, der Betreiber oder der Support in der Sitzung einer anderen Nebenstelle an, sind Chat, Mailbox, Anrufliste, Aufzeichnungen, Berichte, Live-Ansicht und Telefon gesperrt; die Anmeldung steht im Ereignisprotokoll. Einrichten oder Abschalten der Zwei-Faktor-Anmeldung ist in solchen Sitzungen gesperrt.

Support-Aufschaltung (On-Premise):

- Die Anlage des Kunden baut die Verbindung selbst nach außen auf; beim Kunden ist kein Port geöffnet. Erreichbar ist nur die Verwaltung der Anlage, nicht Portal, Datenbank, Vermittlungssoftware oder Betriebssystem.
- Tarif Standard: Zugang nur, nachdem der Kunde ihn in der Verwaltung freigegeben hat, für 24 Stunden, jederzeit sofort beendbar. Tarif Managed: Zugang dauerhaft freigegeben, vom Kunden jederzeit für sieben Tage pausierbar.
- Anmeldung des Supports mit einmaligem Zugangscode (60 Sekunden gültig), Sitzung höchstens acht Stunden. Verbindungsdaten sind über diesen Zugang nicht abrufbar.
- Jede aufgerufene Seite und jede Aktion des Supports steht im Ereignisprotokoll der Anlage des Kunden; jede Aufschaltung steht zusätzlich im Protokoll von KREATIKA.

Trennung:

- Mehrere Kunden teilen sich eine Anlage. Jede Anfrage gilt nur für den eigenen Mandanten; alle Daten hängen über Fremdschlüssel am Mandanten, Dateien liegen in einem Ordner je Mandant.
- Eingehende Anrufe werden nur vermittelt, wenn die Rufnummer dem Mandanten gehört und das SIP-Paket von einer Adresse eines Anbieters dieses Mandanten kommt.

Verschlüsselung:

- Portal und Verwaltung nur über HTTPS; Telefon im Browser und App über verschlüsselten WebSocket, Sprache dort immer mit DTLS-SRTP.
- Tischtelefone von außen über SIP mit TLS (Port 5061), Sprache mit SRTP, soweit das Telefon es unterstützt.
- Benachrichtigungen an Browser und Apps sind je Gerät Ende zu Ende verschlüsselt (RFC 8291), siehe Anlage 4.
- Nicht verschlüsselt sind derzeit: Signalisierung und Sprache zum SIP-Anbieter des Kunden (der Anschluss bei easybell läuft über UDP ohne SRTP; ob verschlüsselt werden kann, hängt vom Anbieter ab), Aufzeichnungen und Sprachnachrichten auf dem Datenträger des Servers, Zugangstoken für Microsoft- und Google-Konten sowie Zugangsdaten der SIP-Anschlüsse in der Datenbank, der Datenträger des Servers und die Datensicherungen. Diese Daten sind durch Zugangskontrolle, Trennung und den Standort im Rechenzentrum geschützt.

Integrität

- Ereignisprotokoll der Verwaltung mit Zeitpunkt, handelnder Person, Vorgang und Mandant.
- Abgewiesene SIP-Anmeldungen, abgewiesene eingehende und ausgehende Anrufe und Sperren werden mit Quelladresse protokolliert.
- Schutz gegen Gebührenbetrug: gesperrte Sondernummern (0900, 0137, 118), freigegebene Länder, Höchstzahl gleichzeitiger Gespräche, Tageslimit für Auslandsgespräche (mit Mail an den Kunden, sobald ein Mailanbieter eingerichtet ist, siehe Anlage 4). Notruf 110 und 112 ist davon ausgenommen.
- Feste Version der Vermittlungssoftware (FreeSWITCH 1.11.3, Abbild mit Prüfsumme).

- Updates der On-Premise-Anlagen sind mit Ed25519 signiert; die Anlage prüft Prüfsumme und Signatur, bevor sie ein Paket einspielt, und legt vorher eine Sicherung an.

Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung des ganzen Systems um 2:30 Uhr auf einen Proxmox Backup Server von KREATIKA auf einem zweiten Server, mit Aufnahmen und Sprachnachrichten. Die Sicherungen werden wöchentlich auf Lesbarkeit geprüft.
- Täglich um 6 Uhr Kopie aller Sicherungen auf eine Hetzner Storage Box (außer Haus, getrennt von beiden Servern).
- Zusätzlich tägliche Sicherung der Datenbank und der Ansagen auf dem Server selbst; jede Sicherung wird vor dem Ablegen gelesen und geprüft und mit Prüfsumme abgelegt.
- Aufbewahrung nach Anlage 2.
- Letzte vollständige Wiederherstellung der Cloud-Anlage aus der Sicherung: 24. Oktober 2026 (Umzug der Anlage auf einen anderen Server über den Proxmox Backup Server).
- Wiederherstellung der Datenbank spielt diese zuerst unter einem zweiten Namen ein und tauscht sie erst, wenn sie vollständig ist.

Verfahren zur Überprüfung

- Änderungen werden vor dem Ausrollen geprüft (Selbsttests der Software, Prüfschritte nach dem Ausrollen). Vor jedem Ausrollen wird die Datenbank gesichert.
- Überprüfung dieser Maßnahmen mindestens einmal jährlich und nach jeder wesentlichen Änderung durch Maximilian A. Grimm, nächste Überprüfung spätestens im November 2027.

Anlage 4: Unterauftragsverarbeiter und Push-Dienste

Unterauftragsverarbeiter

Unternehmen	Leistung	Ort
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server und Rechenzentrum der Cloud-Anlage, des Push-Vermittlers und des Proxmox Backup Servers; Storage Box für die Kopie der Sicherungen außer Haus	Deutschland
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Vertragspartner in der EU: Google Ireland Limited)	Firebase Cloud Messaging: Weckmeldung an die Android-App und an Chrome und Edge	USA
Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA	Apple Push Notification Service: Weckmeldung an die iPhone-App und an Safari	USA

Die Cloud-Anlage versendet derzeit keine E-Mails (kein Mailserver eingerichtet). Sprachnachrichten per Mail und die Mail bei erreichtem Tageslimit für Auslandsgespräche stehen deshalb erst zur Verfügung, wenn KREATIKA einen Mailanbieter einrichtet; dieser wird vorher nach § 5 Abs. 2 mitgeteilt.

Push-Dienste

Damit Telefon im Browser und App bei geschlossenem Fenster klingeln, schickt die Anlage eine Weckmeldung über den Push-Dienst des Geräteherstellers. Das geschieht nur, wenn der Nutzer Benachrichtigungen einschaltet oder die App einrichtet.

Dienst	Wofür
Apple Push Notification Service (Apple Inc., USA)	iPhone-App (VoIP-Push beim Klingeln, stiller Push bei Ende des Anrufs) und Safari
Firebase Cloud Messaging (Google LLC, USA)	Android-App, Chrome und Edge
Mozilla Push Service (Mozilla Corporation, USA)	Firefox
Windows Push Notification Service (Microsoft Corporation, USA)	Edge unter Windows, soweit der Browser diesen Dienst nutzt

Was in der Meldung steht

- Nummer und Name des Anrufers, die Gesprächskennung und die Art des Ereignisses (Klingeln, angenommen, verpasst) liegen immer verschlüsselt in der Meldung, je Gerät mit dessen eigenem Schlüssel (RFC 8291). Der Push-Dienst und der Push-Vermittler können diesen Teil nicht lesen.
- Im Klartext sieht der Push-Dienst die Adresse des Geräts (Token), Größe und Zeitpunkt der Meldung. Bei der App steht zusätzlich ein Anzeigename im Klartext: nur der Name oder die Marke des Kunden, sonst „Eingehender Anruf“, keine Nummer.
- Die Anzeige von Name und Nummer des Anrufers im Klartext (Schalter `PUSH_CALLER_IN_CLEAR`) ist in der Cloud-Anlage ausgeschaltet. Bei On-Premise-Anlagen entscheidet der Kunde; schaltet er sie ein, sehen Apple, Google und der Push-Vermittler Name und Nummer des Anrufers.

Einordnung und Grundlage der Übermittlung

- Apple Push Notification Service und Firebase Cloud Messaging setzt KREATIKA als Herausgeber der Apps selbst ein; sie sind Unterauftragsverarbeiter (siehe oben). Für Firebase gelten die Firebase Data Processing and Security Terms von Google, für Apple das Apple Developer Program License Agreement.
- Die Dienste für Web-Push (Mozilla, Microsoft, Google und Apple für ihre Browser) bestimmt der Browser des Nutzers, nicht KREATIKA. Die Anlage übergibt ihnen nur die verschlüsselte Meldung an die Adresse, die der Browser vorgibt.
- Grundlage der Übermittlung in die USA ist der Angemessenheitsbeschluss der EU-Kommission zum EU-U.S. Data Privacy Framework vom 10. Juli 2023 (Art. 45 DSGVO), unter dem die genannten Anbieter zertifiziert sind. Entfällt er, gelten die Standardvertragsklauseln der EU-Kommission, die die Anbieter in ihre Bedingungen aufgenommen haben (Art. 46 Abs. 2 lit. c DSGVO). Übermittelt werden außer der Geräteadresse, dem Zeitpunkt und der Größe nur verschlüsselte Inhalte.