Technische und organisatorische Maßnahmen (TOM)

Stand: 26.08.2026 · Version 1.1 · Dokumentensatz 2026-08_v1

Geltung

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen der EchoCall LLC nach Art. 32 DSGVO für die Plattform hub.echocall.de. Es ist Anlage 2 des Auftragsverarbeitungsvertrags. Die Maßnahmen werden fortlaufend dem Stand der Technik angepasst, ohne das Schutzniveau zu unterschreiten.

1. Zutritts- und Infrastruktursicherheit

- Betrieb ausschließlich in ISO-27001-zertifizierten Rechenzentren (IONOS, Standorte Deutschland und Frankreich, insbesondere Frankfurt und Karlsruhe) mit den dortigen physischen Sicherheitsmaßnahmen (Zutrittskontrolle, Videoüberwachung, redundante Strom- und Netzanbindung)
- EchoCall-Personal hat keinen physischen Zugang zu den Rechenzentren; der Nachweis physischer Sicherheit erfolgt über die Zertifizierungen des Infrastrukturbetreibers
- Verschlüsselung ruhender Daten auf Storage-Ebene der Infrastruktur (Infrastrukturbetreiber IONOS)

2. Zugangskontrolle (Authentifizierung)

- Passwortlose Anmeldung über zeitlich begrenzte Einmalcodes (Magic Link/Login-Code) oder Passwort-Anmeldung mit bcrypt-gehashten Passwörtern
- Optionale Zwei-Faktor-Authentifizierung (TOTP); 2FA-Geheimnisse werden mit AES-256-GCM verschlüsselt gespeichert, Backup-Codes gehasht
- Session-Verwaltung über signierte, HttpOnly-Cookies; Agent-Sitzungen im Live-Chat über signierte JWT-Token
- Rate Limiting und Sperr-Mechanismen gegen Brute-Force-Versuche, IP-basierte Begrenzung der Registrierung

3. Zugriffskontrolle (Berechtigungen)

- Rollenbasierte Zugriffskontrolle (Kunde, Administrator, Reseller) mit serverseitiger Durchsetzung
- Granulare Workspace-Berechtigungen pro Funktionsbereich für Team-Mitglieder; Einladungs- und Freigabeprozess durch den Kontoinhaber
- Strikte Mandantentrennung auf Datenebene: jede Abfrage ist auf den Eigentümer-Kontext beschränkt; Reseller sehen ausschließlich ihre eigenen Kunden
- Öffentliche API nur mit HMAC-signierten API-Schlüsseln, optional zusätzlich IP- und Domain-Whitelist; vollständiges Request-Logging
- Chat-Widget mit Domain-Whitelist gegen unbefugte Einbettung (fail-closed)

4. Übertragungskontrolle

- Transportverschlüsselung TLS 1.3 (HTTPS erzwungen) für alle Verbindungen zwischen Endgeräten, Plattform und Unterauftragsverarbeitern
- Zugangsdaten von Kundensystemen (Integrationen) werden serverseitig gespeichert und niemals an Sprachmodelle übergeben; Aktionen laufen über einen Webhook-Proxy der Plattform
- SMTP-Zugangsdaten werden verschlüsselt gespeichert (AES-256-CBC); Zahlungsdaten werden ausschließlich beim Zahlungsdienstleister verarbeitet (PCI-DSS), EchoCall speichert keine Kartendaten

5. Eingabe- und Nachvollziehbarkeitskontrolle

- Audit-Logs für sicherheitsrelevante Ereignisse (Anmeldungen, fehlgeschlagene Versuche, administrative Aktionen)
- Protokollierung von Dokumenten- und Rechnungszugriffen
- Registrierungs-Einwilligungen werden mit Zeitstempel und Versionsstand des Rechtsdokumentensatzes gespeichert (Art. 7 Abs. 1 DSGVO)

6. Auftragskontrolle

- Schriftliche Verträge mit allen Unterauftragsverarbeitern nach Art. 28 Abs. 4 DSGVO inklusive Standardvertragsklauseln bei Drittlandbezug
- Versionierte, vertragliche Subprozessorenliste mit Informations- und Widerspruchsverfahren (30 Tage)
- Gesamte Sprachverarbeitung (Spracherkennung, Sprachsynthese, LLM-Inferenz der Standardprofile EchoCall-Voice/EchoCall-Smart) als eigene Software auf eigener EU-Infrastruktur, kein externer Sprach- oder Modell-Dienstleister in der Gesprächskette; optionale externe Modellprofile sind von dieser Zusicherung ausgenommen (Kundenentscheidung)

7. Verfügbarkeitskontrolle

- Redundante Infrastruktur des Rechenzentrumsbetreibers; Verfügbarkeitsziel 99,9 % (Enterprise 99,95 %)
- Regelmäßige Datenbank-Backups; Rechnungsdokumente werden zusätzlich stündlich auf einen separaten Backup-Server gesichert
- Fehler- und Verfügbarkeitsüberwachung (Sentry mit EU-Ingest, Übermittlung personenbezogener Daten deaktiviert), Health-Checks für Integrationen
- Rate Limiting auf Anwendungsebene, DDoS-Basisschutz auf Infrastrukturebene

8. Trennungskontrolle

- Logische Mandantentrennung sämtlicher Kundendaten innerhalb der Plattform
- Whitelabel-Instanzen des Tarifs PartnerNet SaaS Titan werden als separate Instanzen betrieben
- Trennung von Produktions- und Entwicklungsumgebung

9. Datenminimierung, Aufbewahrung und Löschung

- Aufbewahrungsfristen pro Agent konfigurierbar (1/7/30/90/365 Tage, benutzerdefiniert bis 3650 Tage oder unbegrenzt); Standard für neue Agenten: 30 Tage
- Automatisierter täglicher Löschlauf entfernt Transkripte, Aufzeichnungs-Verweise und extrahierte Gesprächsinhalte nach Fristablauf aus allen Speichern der Plattform (Analyse-Datenbank und Gesprächsspeicher der Agenten-Laufzeit)
- Gesprächsaufzeichnung pro Agent deaktivierbar; Zero-PII-Modus verhindert die dauerhafte Speicherung identifizierender Gesprächsinhalte
- DSGVO-Löschfunktion in der Live Inbox mit endgültiger Löschung nach 30 Tagen Karenz
- Vollständige Konto-Löschung entfernt sämtliche Agenten, Wissensdatenbanken, Konversationen, Analytikinhalte und Dateien der Plattform; gesetzlich aufbewahrungspflichtige Rechnungsdaten werden gesperrt und nach Fristablauf gelöscht

10. Incident-Management

- Dokumentierter Prozess zur Erkennung, Bewertung und Behandlung von Sicherheitsvorfällen mit automatisiertem Alerting
- Benachrichtigung betroffener Kunden unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis einer sie betreffenden Verletzung
- Regelmäßige interne Sicherheitsüberprüfungen und Code-Audits; Erkenntnisse fließen dokumentiert in die Plattform ein

Downloads

- TOM als PDF (Deutsch): https://echocall.de/documents/echocall-tom-de.pdf
- TOM as PDF (English): https://echocall.de/documents/echocall-tom-en.pdf

---