AUDICAP · TRUST CENTER

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Stand: 21. Oktober 2026 · Version 1.1 · trust.audicap.app

Verantwortlicher: IMA GmbH · Marketing & Consulting, Heinrich-Barth-Straße 17, 66115 Saarbrücken · Kontakt: privacy@audicap.app

Datenschutzbeauftragter: Anwaltskanzlei Stefan Wiesen, Mainzer Straße 161, 66121 Saarbrücken

---

Geltungsbereich

Diese Maßnahmen gelten für die Verarbeitungen, die die IMA GmbH für Audicap selbst durchführt:

- Websites audicap.app und trust.audicap.app sowie E-Mail (Server bei Hetzner in Falkenstein),
- Konto, Lizenz, Abo-Status, Modell-Downloads, Updates und Support über api.audicap.app (eigener Server der IMA GmbH in Saarbrücken),
- Build, Signatur und Veröffentlichung der App.

Nicht erfasst sind Meeting-Inhalte. Aufnahmen, Transkripte, Zusammenfassungen und Sprecherprofile verarbeitet die App ausschließlich auf dem Gerät des Nutzers oder, wenn der Nutzer das einrichtet, direkt bei dessen eigenem Cloud-Anbieter. Sie gelangen nie zur IMA GmbH. Die Schutzfunktionen der App beschreibt das Trust Center im Abschnitt „App-Sicherheit“.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Website- und Mailserver: Rechenzentrum der Hetzner Online GmbH in Falkenstein. Hetzner ist für Infrastruktur und Betrieb seiner Rechenzentren nach DIN ISO/IEC 27001:2022 zertifiziert (Zertifizierungsstelle SOCOTEC). Den Zutritt regelt Hetzner im Rahmen des Auftragsverarbeitungsvertrags.
- Lizenzserver api.audicap.app: kein Rechenzentrum, sondern ein abgeschlossener Serverraum in den Geschäftsräumen der IMA GmbH in Saarbrücken. Den Schlüssel zum Serverraum hat nur die Geschäftsführung. Die Geschäftsräume sind durch eine Alarmanlage und Videoüberwachung gesichert.

1.2 Zugangskontrolle

- Von außen erreichbar sind nur HTTP und HTTPS über einen Reverse Proxy. HTTP leitet auf HTTPS um, HSTS ist gesetzt. Die Anwendung selbst und die Verwaltungsoberflächen von Proxy und Virtualisierung sind von außen nicht erreichbar.
- Die Administrationsoberfläche des Lizenzservers ist nur aus dem Netz der IMA GmbH erreichbar, von außen wird sie abgewiesen. Sie hat ein Administratorkonto, Passwort mit bcrypt gespeichert, Schutz gegen Cross-Site-Request-Forgery, höchstens zehn Anmeldeversuche pro Stunde und IP-Adresse, ein Sitzungs-Cookie nur über HTTPS und nicht per Skript lesbar, Sitzungsende nach 24 Stunden. Eine Zwei-Faktor-Anmeldung gibt es dort nicht.
- Server-Administration per SSH; als root auf dem Lizenzserver nur mit Schlüssel. Das Netz des Lizenzservers ist für die Administration nur vor Ort oder über ein WireGuard-VPN erreichbar.
- Website-Server: Administration per SSH mit Schlüssel.

- Quellcode bei GitHub: Zwei-Faktor-Anmeldung für alle Personen mit Zugriff.

1.3 Zugriffskontrolle

- Administrativen Zugriff auf die Server haben die Geschäftsführung und eine weitere Person. Die Schlüssel zum Signieren der App hat nur die Geschäftsführung.
- Zugänge werden nur für die jeweilige Aufgabe vergeben. Scheidet jemand aus, entziehen wir am letzten Arbeitstag GitHub-Zugriff, SSH-Schlüssel und Konten und ändern gemeinsam genutzte Passwörter.
- Passwörter von Nutzerkonten werden ausschließlich als bcrypt-Hash (Kostenfaktor 12) gespeichert.
- Anmeldelinks per E-Mail gelten 15 Minuten, Kopplungscodes für die App 2 Minuten. Zugriffstoken gelten 15 Minuten, Erneuerungstoken 30 Tage; Erneuerungstoken, Anmeldelinks, Passwort-Rücksetzungen und Programmschlüssel werden nur als Hash gespeichert.
- Ratenbegrenzung: allgemein 100 Anfragen pro Minute und IP-Adresse, bei Anmeldung und Passwort-Rücksetzung 5 bis 30 Versuche pro 15 Minuten.
- Der Lizenzserver startet nicht mit Standard- oder zu kurzen Geheimnissen; Anmeldetoken, Codes und Zustandsparameter werden in Protokollen geschwärzt.

1.4 Trennungskontrolle

- Website und Lizenzserver laufen auf getrennten Systemen an getrennten Standorten.
- Der Lizenzdienst läuft in einem eigenen Container auf einem eigenen virtuellen System (LXC) mit eigener Datenbank.
- Meeting-Inhalte sind durch die Architektur getrennt: Sie liegen nicht auf Systemen der IMA GmbH.

1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Alle Verbindungen zu audicap.app, trust.audicap.app und api.audicap.app laufen über HTTPS (TLS 1.3 beim Lizenzserver).
- E-Mails von audicap.app sind mit SPF, DKIM und DMARC abgesichert.
- Der Lizenzserver speichert keine Zahlungsdaten, nur eine Kundenreferenz von Stripe.
- Die Kopie der Sicherungen am getrennten Standort liegt verschlüsselt. Der Backup-Server im Haus und die Datenträger des Lizenzservers sind nicht verschlüsselt; sie stehen im abgeschlossenen Serverraum (1.1).
- Entwicklung und automatische Tests arbeiten ohne Produktivdaten. Ein Diagnosepaket holen wir nur zu einer konkreten Support-Anfrage auf einen verschlüsselten Arbeitsrechner und löschen es nach der Analyse.
- Der Build-Rechner für macOS ist mit FileVault verschlüsselt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Programm-Updates werden nur über HTTPS von api.audicap.app ausgeliefert. Die macOS-App ist mit einer Apple Developer ID signiert und von Apple notarisiert, die Windows-App über Microsoft Azure Artifact Signing auf die IMA GmbH signiert. Der Windows-Updater installiert nur Pakete mit dieser Signatur.
- Sprachmodelle prüft die App vor der Nutzung gegen fest hinterlegte SHA-256-Prüfsummen.
- Veröffentlichte Dateien werden beim Hochladen per SHA-256 geprüft; jede Veröffentlichung endet mit einer Prüfung, dass die öffentlich ausgelieferten Dateien dem abgenommenen Stand entsprechen.

2.2 Eingabekontrolle

- Änderungen am Code laufen über die Versionsverwaltung Git; Änderungen am Lizenzserver werden vor dem Einspielen gegen den versionierten Stand verglichen.
- Der Lizenzserver protokolliert Anfragen mit Zeitpunkt und IP-Adresse (Aufbewahrung siehe 5.).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Lizenzserver: tägliche Sicherung im laufenden Betrieb auf einen Backup-Server im Haus (eigene virtuelle Maschine auf gespiegelten Platten) und jede Nacht eine Kopie an einen räumlich getrennten Standort. An beiden Orten bleiben 14 tägliche, 8 wöchentliche, 12 monatliche und 3 jährliche Stände. Die Lesbarkeit der Sicherungen wird wöchentlich geprüft; eine Überwachung meldet, wenn eine Sicherung älter als 26 Stunden ist.
- Wiederherstellung: Höchstens die Daten seit der letzten nächtlichen Sicherung gehen verloren (bis zu 24 Stunden). Ziel für die Wiederherstellung des Lizenzservers sind drei Werktage. Die Wiederherstellung wird jährlich in einer abgetrennten Testumgebung geprüft, zuletzt am 19. Oktober 2026 (Dienst betriebsbereit, Datenbank vollständig, Prüfsummen identisch).
- Website-Server: tägliche Sicherung, lokal und extern. Die Website selbst liegt zusätzlich vollständig in der Versionsverwaltung.
- Der Lizenzdienst meldet seinen Zustand alle 30 Sekunden; beendet er sich unerwartet, startet Docker ihn automatisch neu.
- Eine Überwachung prüft api.audicap.app jede Minute und benachrichtigt bei einem Ausfall und vor Ablauf des Zertifikats per Push-Nachricht.
- Fällt der Lizenzserver aus, arbeitet die App weiter: Eine erfolgreich geprüfte Lizenz gilt 14 Tage ohne Verbindung.
- Sicherheitsupdates des Betriebssystems spielen Lizenzserver und Virtualisierungs-Host automatisch ein; Virtualisierungssoftware und Container werden von Hand aktualisiert.
- Der Serverraum hat Rauchmelder und Klimatisierung. Eine unterbrechungsfreie Stromversorgung gibt es nicht.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Diese Maßnahmen werden jährlich und bei jeder größeren Änderung der Infrastruktur überprüft.
- Alle Personen mit Zugriff sind auf Vertraulichkeit verpflichtet.
- Datenschutzbeauftragter ist die Anwaltskanzlei Stefan Wiesen, Saarbrücken.
- Verletzungen des Schutzes personenbezogener Daten bewertet die Geschäftsführung unverzüglich zusammen mit dem Datenschutzbeauftragten. Meldepflichtige Fälle melden wir innerhalb von 72 Stunden an das Unabhängige Datenschutzzentrum Saarland, bei hohem Risiko benachrichtigen wir die Betroffenen (Art. 33 und 34 DSGVO). Jeder Vorfall wird dokumentiert.
- Schwachstellen nimmt security@audicap.app entgegen; Meldeweg und Fristen regelt die öffentliche Richtlinie unter audicap.app/sicherheit.html, maschinenlesbar nach RFC 9116.
- Unterauftragsverarbeiter werden im Trust Center geführt; Änderungen kündigen wir vorab per E-Mail an.

5. Datenschutz durch Technikgestaltung und Löschung (Art. 25 DSGVO)

- Meeting-Inhalte bleiben auf dem Gerät; neue Installationen nutzen standardmäßig lokale Modelle.
- Absturzberichte, Zugriff für KI-Assistenten und Handy-Empfang sind standardmäßig aus.

- Ein Diagnosepaket wird einer Support-Anfrage nur angehängt, wenn der Nutzer es ausdrücklich ankreuzt; es wird nach 90 Tagen gelöscht.
- Abgelaufene Token und Codes löscht der Lizenzserver alle sechs Stunden.
- Protokolle der Anwendung werden nach 30 Tagen gelöscht, Zugriffsprotokolle des Reverse Proxy nach spätestens fünf Wochen, seine Fehlerprotokolle nach spätestens elf Wochen. Protokolle der Websites werden täglich rotiert und nach spätestens 30 Tagen gelöscht (derzeit nach zehn Tagen).
- Download-Protokolle (IP-Adresse, Browser- bzw. Programmkennung) werden auf 30 Tage begrenzt; die automatische Löschung ist beauftragt, bis dahin wird von Hand gelöscht.
- Support-Anfragen werden auf Verlangen gelöscht, sofern keine Aufbewahrungspflicht besteht. Konten lassen sich in der App löschen (ab Version 0.13.0) oder auf Anfrage; laufende Abos werden dabei gekündigt.