

Technische und organisatorische Maßnahmen

Stand 06.08.2026 · Version 1.0

Anbieter audyra UG (haftungsbeschränkt) i. G., Koskauer Straße 20, 07922 Tanna

Vertretung Mario Moreno, Ronny Krupsky · Kontakt info@simokru.de · +49 1512 9533086

Entwurfsstand. Die Maßnahmen sind so zu dokumentieren, wie sie tatsächlich umgesetzt sind. Vor Weitergabe an Kunden ist jede Zeile gegen den realen Betriebszustand zu prüfen — eine TOM, die mehr beschreibt als umgesetzt ist, ist ein Haftungsrisiko und im Prüfungsfall schwerer zu rechtfertigen als eine knappe, zutreffende Darstellung.

1 Vertraulichkeit

1.1 Zutrittskontrolle

Der Betrieb erfolgt in Rechenzentren der Hetzner Online GmbH in Frankfurt am Main und Nürnberg. Der physische Zutritt wird durch den Betreiber gesichert (Vereinzelungsanlage, Videoüberwachung, protokollierte Zutrittsberechtigungen). Eigene Serverräume werden nicht betrieben.

1.2 Zugangskontrolle

- Anmeldung ausschließlich über verschlüsselte Verbindungen (TLS)
- Kennwörter werden nicht im Klartext gespeichert, sondern als Hash mit Salt abgelegt
- Mehr-Faktor-Authentifizierung ist für administrative Rollen verpflichtend und für alle übrigen Rollen aktivierbar
- Automatische Abmeldung nach Inaktivität
- Administrativer Serverzugang nur über Schlüsselpaare, keine Kennwörter

1.3 Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept innerhalb des Mandanten
- **Mandantentrennung als Row-Level-Security in der Datenbank.** Die Trennung wird auf Ebene der Datenbank erzwungen, nicht durch eine Bedingung in der Anwendungsabfrage. Ein Fehler in der Anwendungsschicht führt damit nicht zu einem Datenabfluss zwischen Mandanten.
- Zugriffe auf Nachweisdokumente werden protokolliert

1.4 Trennungskontrolle

Daten unterschiedlicher Verantwortlicher werden logisch getrennt verarbeitet. Test- und Produktivumgebung sind getrennt; Produktivdaten werden nicht in Testumgebungen verwendet.

1.5 Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung durchgehend über TLS
- Verschlüsselung der Datenträger im Ruhezustand
- Sicherungskopien verschlüsselt abgelegt

2 Integrität

2.1 Weitergabekontrolle

Eine Übermittlung an Dritte erfolgt nur an die in Anlage 2 der Auftragsverarbeitung genannten Stellen. Datenexporte durch den Verantwortlichen werden protokolliert.

2.2 Eingabekontrolle

- Jede eingebende und ändernde Handlung wird mit Benutzer, Zeitpunkt und Vorgang protokolliert
- **Das Protokoll ist als Hash-Kette geführt:** jeder Eintrag enthält die Prüfsumme des vorhergehenden. Eine nachträgliche Änderung eines Eintrags führt dazu, dass die Kette nicht mehr aufgeht und auffällt.
- Freigegebene Dokumente werden mit einer Signatur nach eIDAS im Format PAdES-B-B versehen. Die Unversehrtheit lässt sich ohne Zugang zur Anwendung prüfen.
- Korrekturen erfolgen als Ergänzung, nicht durch Überschreiben

3 Verfügbarkeit und Belastbarkeit

- Tägliche automatisierte Sicherung der Datenbank
- Getrennte Aufbewahrung der Sicherungen vom Produktivsystem
- Wiederherstellung wird regelmäßig erprobt und das Ergebnis dokumentiert
- Überwachung der Erreichbarkeit mit Benachrichtigung bei Störungen
- Schutzmaßnahmen gegen Überlastangriffe durch den Rechenzentrumsbetreiber
- Einspielen sicherheitsrelevanter Aktualisierungen nach Bewertung der Dringlichkeit

Zu ergänzen, sobald festgelegt. Aufbewahrungsdauer der Sicherungen, angestrebte Wiederherstellungszeit und maximal zulässiger Datenverlust. Ohne diese Werte ist die Zeile „Wiederherstellung wird erprobt“ für einen Kunden nicht bewertbar.

4 Verfahren zur regelmäßigen Überprüfung

- Überprüfung dieser Maßnahmen mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen
- Verpflichtung der Beschäftigten auf Vertraulichkeit und Unterweisung im Datenschutz
- Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten ist eingerichtet
- Auswahl von Unterauftragsverarbeitern nach dokumentierten Kriterien

5 Datenschutzfreundliche Voreinstellungen

- Neue Benutzer erhalten die Rolle mit dem geringsten erforderlichen Berechtigungsumfang
- Bei der Bildauswertung werden die Inhalte beim eingesetzten Dienst nicht gespeichert und nicht zu Trainingszwecken genutzt
- Module, die besondere Kategorien personenbezogener Daten verarbeiten, sind standardmäßig nicht aktiv und ohne Offline-Erfassung ausgelegt

6 Änderungsverzeichnis

Version	Stand	Änderung
1.0	06.08.2026	Erstfassung