Technische und organisatorische Maßnahmen

ELMİ · Dokumentierter Stand vom 8. Oktober 2026

Technischer Ist-Stand, keine Zertifizierung.
Dieses Dokument trennt überprüfte Maßnahmen von noch offenen vertraglichen und organisatorischen Punkten. Als verbindliche AVV-Anlage ist es erst nach deren Klärung und ausdrücklicher Vereinbarung zu verwenden.

1. System und Datenhaltung

Die produktive Anwendung, Datenbank und hochgeladenen Nachweise werden auf einem Hetzner-Server in Falkenstein, Deutschland betrieben. Die Kommunikation mit der Webanwendung erfolgt über HTTPS. Zusätzliche E-Mail-, Zahlungs- und KI-Dienste sind gesondert zu betrachten; deren Verarbeitung ist nicht pauschal auf Deutschland beschränkt.

Die Anwendung läuft mit einem eigenen Betriebssystembenutzer. Das produktive Datenverzeichnis ist durch Betriebssystemberechtigungen gegen Zugriff anderer gewöhnlicher Benutzer geschützt. Dies ist keine Verschlüsselung der Datenbank oder aller Mediendateien im Ruhezustand.

2. Anmeldung und Berechtigungen

Anwendungsschnittstellen prüfen die jeweilige Rolle, den Mandanten und gegebenenfalls konkrete Objekt-/Kontozuordnungen serverseitig. Auftraggeber, Mitarbeiter, Verwaltung und Betreiber haben getrennte Berechtigungsmodelle. Interne Vergütungsdaten sind auf Inhaber und ausdrücklich berechtigte Verwaltung begrenzt.

Passwörter werden als gesalzene Hashes verarbeitet. Anmeldungen und Wiederherstellungsabläufe haben zeitliche Begrenzungen sowie Maßnahmen gegen wiederholte Fehlversuche. Der Betreiberzugang ist zusätzlich durch Mehrfaktor-Authentifizierung geschützt. Einrichtbare Passkeys geben keine biometrischen Rohdaten an ELMİ weiter.

Verwaltungssitzungen können bei berechtigter Nutzung bis zu 30 Tage weitergelten und werden widerrufbar geführt. Die persönliche Geräteübersicht zeigt nur die eigenen Sitzungen. Es wird keine verpflichtende Mehrfaktor-Authentifizierung für sämtliche Anwender behauptet.

3. Schutz ausgewählter Geheimnisse

Ausgewählte Anbieterzugänge und vergleichbare Geheimnisse werden auf Anwendungsebene mit AES-GCM verschlüsselt. Diese Maßnahme ist zweckbezogen und darf nicht als Ende-zu-Ende-Verschlüsselung aller Kundeninhalte beschrieben werden. Zugriff auf Betriebsschlüssel bleibt auf den Serverbetrieb begrenzt.

Datentrennung und Nachvollziehbarkeit

TOM · nachgewiesene Anwendungsmaßnahmen

4. Öffentliche und interne Daten

Öffentliche Objektseiten und der Kundenbereich verwenden reduzierte serverseitige Datenansichten. Arbeitsbeginn, Arbeitsende und Einsatzdauer verbleiben in der internen Verwaltung. Personen werden in externen Nachweisen mit gekürztem Nachnamen dargestellt.

Öffentlich freigegebene Leistungsdaten und Unterschriften bleiben personenbezogen. Der Verantwortliche muss deren Veröffentlichung rechtlich prüfen und Betroffene informieren. Interne Kontrollergebnisse werden nicht durch bloßes Öffnen eines öffentlichen Links vollständig freigegeben.

Standort wird bei bewussten Buchungsschritten angefragt; ein dauerhaftes Bewegungsprofil wird nicht erzeugt. Eine konfigurierte Standortpflicht ist eine Entscheidung der zuständigen Verwaltung.

5. Änderungen und Freigaben

Sicherheitsrelevante Betreiberaktionen sowie wesentliche Verwaltungskorrekturen besitzen dokumentierte Prüf- beziehungsweise Änderungsspuren. Historische Zeit-/Aufgabenstände und Signaturherkunft werden bei unterstützten Korrekturen getrennt berücksichtigt. Protokolle ersetzen keine rechtliche Beschäftigteninformation.

Vor Veröffentlichungen werden zielbezogene automatisierte Tests, isolierte Laufzeitprüfungen und Bestandsdatenprüfungen eingesetzt. Neue Funktionen werden mit synthetischen Daten geprüft. Ein erfolgreicher Softwaretest wird nicht als Zertifizierung des Gesamtbetriebs ausgegeben.

6. Sicherung und Wiederherstellung

Der Veröffentlichungsablauf erstellt konsistente Sicherungen der Datenbank, Medien und benötigten Installationsdaten. Schreibende Prozesse werden für die konsistente Aufnahme angehalten. Das Sicherungswerkzeug prüft Datenbankintegrität, Dateibestand und Prüfsummen. Sicherungsverzeichnisse sind zugriffsbeschränkt.

Veröffentlichungssicherungen liegen zusätzlich auf dem Anwendungsserver. Der getrennte Sicherungsspeicher schützt gegen Verlust des einzelnen Anwendungsservers, liegt jedoch beim selben Anbieter und am selben Standort. Es wird kein geographisch getrenntes oder unveränderliches Archiv behauptet. Seit 08.10.2026 besteht zusätzlich eine täglich um 03:15 Uhr (Europe/Berlin) geplante, vor Übertragung verschlüsselte Sicherung auf einer getrennten Hetzner Storage Box in Falkenstein. Sie umfasst Datenbank, Medien, Installationsnachweise und Betriebskonfiguration. Die erste Sicherung und vollständige isolierte Wiederherstellung mit Prüfsummen- und Datenbankkontrolle wurden am 08.10.2026 erfolgreich geprüft. Eine automatische Wiederherstellungsprüfung läuft sonntags um 04:15 Uhr. Eine feste Wiederanlaufzeit wird nicht zugesichert.

Betrieb und Anbieter

TOM · Stand und ausstehender Zoho-Nachweis

7. Vertragspartner und externe Verarbeitung

Kontobezogene AVVs/DPAs und das konkrete Anbieterverzeichnis müssen vollständig abgelegt werden. Der Hetzner-AVV vom 08.10.2026 ist intern nachgewiesen. Der tatsächliche Zoho-Abschluss ist noch zu bestätigen; die OpenAI-API-Bedingungen beziehen einen DPA ein, die konkrete API-Kontozuordnung KIR SERVICE wurde anhand Kontoansicht und API-Organisationsprüfung nachgewiesen.

Für optionale KI-Funktionen und E-Mail-Kommunikation sind Datenumfang, Empfänger, Verarbeitungsorte und mögliche Drittlandtransfers je beauftragter Funktion zu bestimmen. Der Download dieser TOMs schließt keine zusätzlichen Anbietervereinbarungen.

8. Löschung und Datensicherung

Die Anwendung bietet Löschabläufe und funktionsbezogene Aufbewahrungsregeln. Neue externe Sicherungen und neue Veröffentlichungssicherungen haben eine 30-Tage-Rotation. Bereits bestehende interne Veröffentlichungssicherungen werden nicht rückwirkend gelöscht. Für aktive Auftragsdaten gilt die Rückgabe-/Löschweisung nach Auftragsende; Umsetzung innerhalb von 30 Tagen. Der minimale Vertragsnachweis ist von Beschäftigtendaten getrennt und hat eine eigene begrenzte Aufbewahrung.

Die externe Sicherung nutzt einen eigenen SSH-Schlüssel, geprüfte Serveridentität, SFTP und Restic-Verschlüsselung. Betriebsschlüssel und Sicherungspasswort sind zugriffsbeschränkt; Wiederherstellungsdaten liegen außerhalb des Webzugriffs. Zeitgeber und Status weisen Sicherungsfehler aus. Wiederherstellungen erfolgen zunächst isoliert; dokumentierte Löschungen sind vor Freigabe erneut anzuwenden. Feste Wiederanlaufzeiten und ein Schutz gegen Kompromittierung aller Betriebsschlüssel werden nicht behauptet.

9. Organisatorische Zuständigkeit

Datenschutzkontakt ist Ömer Kir, handelnd unter ELMİ, kontakt@myelmi.com. Für Zugriffsvergabe, Vertraulichkeitsverpflichtungen, Vorfallbearbeitung, Weisungen, regelmäßige Kontrollen und Löschfreigaben sind Verantwortliche und Nachweise in der Betriebsdokumentation verbindlich zu führen.

Bei der Prüfung wurden nicht sämtliche internen Organisationsnachweise oder die Rechenzentrumsmaßnahmen unabhängig auditiert. Diese Punkte dürfen erst nach Prüfung als zugesicherte Maßnahmen bezeichnet werden.

Prüfumfang und Fortschreibung

Grundlage sind der vorhandene ELMİ-Quellcode, der dokumentierte Veröffentlichungsablauf und eine lesende Prüfung der Produktionskonfiguration am 8. Oktober 2026. Keine Kundendaten wurden für diese Dokumentation verändert. Das Dokument wird bei wesentlichen technischen oder organisatorischen Änderungen versioniert.

Diese TOMs sind gemeinsam mit dem AVV und Anbieterverzeichnis zu bewerten. Sie bescheinigen keine vollständige DSGVO-Konformität.