Technische und organisatorische Maßnahmen

TOM-Version 1.0
Gültig ab 04.08.2026
Anlage zur FindTime-AVV

Die Maßnahmen werden risikoorientiert betrieben und entsprechend technischer Entwicklung, Bedrohungslage und Funktionsumfang überprüft. Sicherheitsdetails, deren Veröffentlichung selbst ein Risiko schaffen würde, werden nur im erforderlichen Umfang offengelegt.

1. Organisation und Verantwortlichkeiten

- klar geregelte administrative Zuständigkeiten;
- Verpflichtung auf Vertraulichkeit und Datengeheimnis;
- regelmäßige Überprüfung von Berechtigungen und sicherheitsrelevanten Änderungen;
- Dokumentation zentraler Änderungen und administrativer Vorgänge im Audit-Protokoll;
- definierte Abläufe für Sicherheitsvorfälle, Wiederherstellung und Datenschutzanfragen.

2. Zutritts- und Infrastrukturschutz

- Betrieb bei einem professionellen Hostinganbieter in Österreich;
- physische Sicherheitsmaßnahmen des Rechenzentrums und kontrollierter Zutritt durch den Hostinganbieter;
- redundante Stromversorgung, technische Überwachung und Schutzmaßnahmen des Rechenzentrums;
- keine öffentliche Bereitstellung von Konfigurations-, Log- und Sicherungsdateien.

3. Zugangskontrolle

- individuelle Benutzerkonten und rollenbasierte Zugriffe;
- Passwörter werden nicht im Klartext gespeichert, sondern mit sicheren Passwort-Hashverfahren verarbeitet;
- sichere Sitzungs-Cookies mit HttpOnly, Secure bei HTTPS und SameSite;

- Schutz sensibler Administrationsbereiche durch Authentifizierung und Rollenprüfung;
- CSRF-Schutz für schreibende Aktionen;
- zeitlich beschränkte und zufällige Einladungs- und Rücksetz-Token.

4. Zugriffskontrolle und Mandantentrennung

- logische Trennung der Mandanten über tenant_id und zentrale Zugriffskontrollen;
- Rollen für Super-Admin, Firmeninhaber, Administratoren und weitere Benutzer;
- Prepared Statements für Datenbankzugriffe;
- kontextbezogene Prüfung von Mandant und Benutzer bei fachlichen Aktionen;
- Protokollierung wichtiger administrativer Änderungen.

5. Übertragungskontrolle

- verschlüsselte Übertragung über HTTPS/TLS;
- System-E-Mails ausschließlich an die im Prozess vorgesehenen Empfänger;
- keine absichtliche Weitergabe von Kundendaten an cron-job.org; Cron-Endpunkte liefern nur technische Statussummen;
- geheime Cron-Schlüssel zur Absicherung zeitgesteuerter Endpunkte;
- Downloads und Exporte nur für berechtigte Benutzer.

6. Eingabe- und Änderungskontrolle

- Audit-Logging für relevante Änderungen;
- Zeitstempel für Erstellung, Aktualisierung, Bestellungen, Freischaltungen und Kündigungen;
- serverseitige Validierung von Eingaben;
- HTML-Ausgabe wird kontextgerecht maskiert;
- Protokollierung der Zustimmung zu rechtlichen Dokumenten mit Version und Zeitpunkt.

7. Verfügbarkeitskontrolle

- regelmäßige Datenbanksicherungen und Downloadmöglichkeit im Super-Admin-Bereich;
- Hosting-Infrastruktur mit Überwachung und Redundanzmaßnahmen;
- Fehlerprotokollierung und kontrollierte Cron-Prozesse;

- Wiederherstellung anhand geprüfter Backups;
- Schutz vor unbeabsichtigter Löschung durch abgestufte Deaktivierungs- und Kündigungsprozesse.

8. Trennungsgebot

- Mandantenbezogene Daten werden logisch getrennt verarbeitet;
- Test-, aktive und beendete Lizenzzustände werden getrennt geführt;
- Verarbeitungen für eigene Verwaltungszwecke werden von der Verarbeitung der Kundendaten im Auftrag unterschieden;
- Konfigurationen und Zugriffsrechte werden je Mandant gespeichert.

9. Datenschutz durch Technikgestaltung

- datensparsame Pflichtfelder;
- keine Zahlungsdaten während des kostenlosen Tests;
- Honeypot und pseudonymisierter IP-Prüfwert zur Missbrauchsabwehr;
- mandantenspezifische Datenschutzinformation auf Buchungsseiten;
- konfigurierbare Rollen, Standorte, Ressourcen und Benachrichtigungen.

10. Wartung und Schwachstellenmanagement

- regelmäßige Aktualisierung der Anwendung und verwendeter Laufzeitumgebungen;
- zeitnahe Behandlung sicherheitsrelevanter Fehler;
- Änderungen werden vor Auslieferung auf Syntax und Kernfunktionen geprüft;
- Konfigurationsgeheimnisse liegen außerhalb öffentlich zugänglicher Ausgaben und werden durch Serverregeln geschützt.

11. Incident Response

- Erfassung und Bewertung von Sicherheitsereignissen;
- Eindämmung, Beweissicherung und Wiederherstellung;
- Information betroffener Verantwortlicher ohne unangemessene Verzögerung;
- Dokumentation von Ursache, Auswirkungen und Abhilfemaßnahmen;
- Nachbereitung zur Vermeidung gleichartiger Vorfälle.

12. Löschung

Nach Vertragsende wird die Verarbeitung eingeschränkt und der Zugang gesperrt. Produktivdaten werden nach dem veröffentlichten Löschkonzept gelöscht oder exportiert. Sicherungskopien werden im regulären Zyklus überschrieben. Gesetzliche Aufbewahrungspflichten für Vertrags-, Abrechnungs- und Nachweisdaten bleiben unberührt.