Technische und organisatorische Maßnahmen

Dokumentversion: 2026-06-12

Stand: 2026-06-12

Anbieter: Stefan Keller – The SysAdminHub

Technische und organisatorische Maßnahmen

Stand: 2026-06-12

Anlage – Technische und organisatorische Maßnahmen (TOM)
zur Auftragsverarbeitung gemäß Art. 28 DSGVO
für die SaaS-Anwendung „Datenschutz-Cloud“

Stand: 11.06.2026

Auftragsverarbeiter:

Stefan Keller – The SysAdminHub
Stefan Keller
Sonthofer Str. 2
87527 Sonthofen
Deutschland

E-Mail: support@datenschutz-cloud.eu

Produkt: Datenschutz-Cloud

1. Allgemeine Beschreibung der technischen Umgebung

Die Datenschutz-Cloud wird als webbasierte SaaS-Anwendung betrieben.

Die Anwendung wird auf einem VPS bei STRATO in Deutschland betrieben. Als Betriebssystem wird Ubuntu eingesetzt. Der Webzugriff erfolgt über nginx als Webserver bzw. Reverse Proxy.

Die Datenhaltung erfolgt über MySQL 8. Hochgeladene Dateien werden im Dateisystem bzw. in persistenten Docker Volumes gespeichert.

Der Zugriff auf die Anwendung erfolgt über HTTPS/TLS. Die TLS-Zertifikate werden über Let's Encrypt bereitgestellt.

2. Zugangskontrolle

Ziel:
Verhinderung des unbefugten Zugangs zu Systemen, auf denen personenbezogene Daten verarbeitet werden.

Maßnahmen:

- Betrieb der Anwendung auf Serverinfrastruktur in Deutschland.
- Administrativer Serverzugriff ausschließlich über SSH.
- SSH-Zugriff erfolgt über SSH-Schlüssel.
- Passwortbasierter SSH-Login ist deaktiviert.
- Direkter Root-Login per SSH ist deaktiviert.
- Zugriff auf administrative Systeme ist auf berechtigte Administratoren beschränkt.
- Firewall ist aktiv und beschränkt den Netzwerkzugriff auf erforderliche Dienste.
- Webzugriff auf die Anwendung erfolgt ausschließlich über verschlüsselte HTTPS/TLS-Verbindungen.
- TLS-Zertifikate werden über Let's Encrypt bereitgestellt.

- Zugriff auf Backup- und Administrationssysteme ist auf berechtigte Administratoren beschränkt.

3. Zugriffskontrolle

Ziel:
Verhinderung unbefugter Nutzung personenbezogener Daten innerhalb der Anwendung.

Maßnahmen:

- Nutzung der Datenschutz-Cloud erfolgt über individuelle Benutzerkonten.
- Benutzer authentifizieren sich mit E-Mail-Adresse bzw. Benutzerkennung und Passwort.
- Passwörter werden nicht im Klartext gespeichert.
- Zwei-Faktor-Authentifizierung ist optional verfügbar.
- Rollen- und Berechtigungskonzept innerhalb der Anwendung.
- Vorhandene Rollen umfassen insbesondere Superuser, Admin, Auditor und User.
- Berechtigungen werden rollenbasiert vergeben.
- Inaktive Benutzerkonten können deaktiviert werden.
- Deaktivierte Benutzer können sich nicht mehr anmelden.
- Zugriff auf Mandantendaten ist an Benutzerrolle und Mandantenzuordnung gebunden.
- Serverseitige Berechtigungsprüfungen schützen Fachseiten und Aktionen.
- Support- und Administrationszugriff auf Kundendaten erfolgt nur zweckgebunden, insbesondere für Support, Fehleranalyse, Wartung, Sicherheit oder auf Weisung des Kunden.
- Administrative Zugriffe werden soweit technisch möglich protokolliert.

4. Mandantentrennung / Trennungskontrolle

Ziel:
Sicherstellung, dass Daten unterschiedlicher Kunden getrennt verarbeitet werden.

Maßnahmen:

- Die Datenschutz-Cloud ist mandantenfähig aufgebaut.
- Fachliche Daten sind einem Mandanten zugeordnet.
- Zugriff auf Mandantendaten erfolgt über Mandantenkontext und rollenbasierte Berechtigungen.
- Serverseitige Prüfungen verhindern unberechtigten Zugriff auf Daten anderer Mandanten.
- Superuser-Funktionen sind vom normalen Mandantenbereich getrennt.
- Mandantenbezogene Daten können über Exportfunktionen getrennt exportiert werden.
- Benutzer werden Mandanten zugeordnet.
- Rollen werden bei Anzeige, Bearbeitung und Verwaltung von Daten berücksichtigt.
- Mandantendaten werden logisch voneinander getrennt verarbeitet.

5. Weitergabekontrolle

Ziel:

Sicherstellung, dass personenbezogene Daten bei Übertragung oder Weitergabe geschützt werden.

Maßnahmen:

- Webzugriffe erfolgen über HTTPS/TLS.
- Administrativer Zugriff erfolgt über SSH.
- Backups werden über eine verschlüsselte Verbindung, insbesondere per SFTP, übertragen.
- Personenbezogene Daten werden nicht ohne Rechtsgrundlage an Dritte weitergegeben.
- Unterauftragnehmer werden nur eingesetzt, soweit dies für Betrieb, Hosting, E-Mail-Versand, Backup oder technische Bereitstellung erforderlich ist.
- Mit relevanten Unterauftragnehmern werden, soweit erforderlich, Verträge zur Auftragsverarbeitung abgeschlossen.
- Eine Drittlandübermittlung ist nicht vorgesehen.
- Kundendaten werden nicht zu eigenen Zwecken des Auftragsverarbeiters verwendet.
- Zugriff auf Kundendaten durch den Auftragsverarbeiter erfolgt nur, soweit dies zur Vertragserfüllung oder zur Sicherheit und Stabilität des Dienstes erforderlich ist.

6. Eingabekontrolle

Ziel:
Nachvollziehbarkeit, ob und von wem personenbezogene Daten eingegeben, geändert oder gelöscht wurden.

Maßnahmen:

- Die Anwendung verfügt über Auditlog- und Systemlog-Funktionen.
- Fachliche Änderungen an zentralen Datenschutzobjekten werden protokolliert, soweit technisch umgesetzt.
- Sicherheitsrelevante Ereignisse können protokolliert werden.
- Login-Ereignisse und fehlgeschlagene Anmeldeversuche können systemseitig erfasst werden.
- Änderungen an wichtigen Objekten wie Verarbeitungstätigkeiten, TOMs, Dienstleistern, DSFA, Maßnahmen, Auditdaten, Vorfällen und Dokumenten können nachvollzogen werden.
- Protokolle enthalten, soweit erforderlich, Zeitstempel, Benutzerbezug, Mandantenbezug und Art der Änderung.
- Protokolldaten werden nur für Sicherheits-, Nachweis- und Fehleranalysezwecke verwendet.
- Zugriff auf Protokolldaten ist auf berechtigte Benutzer beschränkt.

7. Auftragskontrolle

Ziel:
Sicherstellung, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

Maßnahmen:

- Verarbeitung erfolgt auf Grundlage des Hauptvertrags und des Auftragsverarbeitungsvertrags.
- Verarbeitung erfolgt ausschließlich zur Bereitstellung und zum Betrieb der Datenschutz-Cloud.
- Kunden bleiben Verantwortliche für die von ihnen eingegebenen Daten.

- Der Auftragsverarbeiter verarbeitet Kundendaten nicht zu eigenen Zwecken.
- Weisungen können in Textform, insbesondere per E-Mail, erteilt werden.
- Mitarbeitende bzw. berechtigte Personen des Auftragsverarbeiters werden zur Vertraulichkeit verpflichtet.
- Unterauftragnehmer werden dokumentiert.
- Mit Unterauftragnehmern werden, soweit erforderlich, Auftragsverarbeitungsverträge geschlossen.
- Supportzugriffe erfolgen nur zweckgebunden und soweit erforderlich.

8. Verfügbarkeitskontrolle

Ziel:
Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust sowie Sicherstellung der Wiederherstellbarkeit.

Maßnahmen:

- Betrieb der Anwendung auf VPS-Infrastruktur in Deutschland.
- Einsatz von MySQL 8 als Datenbank.
- Speicherung von Datei-Uploads im Dateisystem bzw. in persistenten Docker Volumes.
- Tägliche Datensicherungen der produktiven Daten.
- Backup-Verwaltung über Backrest.
- Technische Backup-Basis ist restic.
- Backups werden in einem restic-Repository verschlüsselt gespeichert.
- Backup-Übertragung zum Backup-Ziel erfolgt über verschlüsselte Verbindung, insbesondere per SFTP.
- Backup-Ziel befindet sich bei Hetzner innerhalb der EU.
- Backup-Aufbewahrung beträgt derzeit bis zu 3 Monate.
- Regelmäßige Restore-Tests werden durchgeführt.
- Zugriff auf Backup-Systeme ist auf berechtigte Administratoren beschränkt.
- Backups dienen der Wiederherstellung des Systembetriebs bei technischen Störungen, Datenverlust oder Sicherheitsvorfällen.
- Eine Wiederherstellung einzelner Kundendaten erfolgt nur, soweit technisch möglich und zur Vertragserfüllung erforderlich.

9. Verschlüsselung und Schutz der Vertraulichkeit

Ziel:
Schutz personenbezogener Daten vor unbefugter Kenntnisnahme.

Maßnahmen:

- Webzugriff auf die Anwendung über HTTPS/TLS.
- TLS-Zertifikate über Let's Encrypt.
- Administrativer Zugriff über SSH mit Schlüssel-Authentifizierung.
- Passwortbasierter SSH-Zugriff ist deaktiviert.

- Root-Login per SSH ist deaktiviert.
- Backups werden durch restic verschlüsselt gespeichert.
- Übertragung von Backups über verschlüsselte Verbindung.
- Passwörter der Anwendung werden nicht im Klartext gespeichert.
- Zugangsdaten und Backup-Schlüssel werden vertraulich behandelt.
- Administrative Zugangsdaten werden nicht im Quellcode gespeichert.
- Zugriff auf produktive Systeme ist auf berechtigte Administratoren beschränkt.

10. Integrität

Ziel:
Schutz personenbezogener Daten vor unbeabsichtigter oder unbefugter Veränderung.

Maßnahmen:

- Zugriff auf Fachfunktionen wird rollenbasiert beschränkt.
- Serverseitige Validierungen und Berechtigungsprüfungen.
- Auditlog für relevante fachliche Änderungen.
- Systemlog für technische und sicherheitsrelevante Ereignisse.
- Backups ermöglichen Wiederherstellung bei Datenverlust oder beschädigten Datenbeständen.
- Regelmäßige Restore-Tests unterstützen die Überprüfung der Wiederherstellbarkeit.
- Änderungen an produktiven Systemen erfolgen nur durch berechtigte Administratoren.
- Schutz administrativer Zugänge durch SSH-Schlüssel und deaktivierten Passwortlogin.

11. Belastbarkeit der Systeme

Ziel:
Sicherstellung eines stabilen technischen Betriebs.

Maßnahmen:

- Betrieb auf VPS-Infrastruktur.
- Einsatz bewährter Komponenten wie Ubuntu, nginx, MySQL 8 und Docker/persistente Volumes.
- Firewall zur Beschränkung unnötiger Netzwerkzugriffe.
- Regelmäßige Backups.
- Protokollierung technischer und sicherheitsrelevanter Ereignisse.
- Möglichkeit zur Wiederherstellung aus Backups.
- Durchführung regelmäßiger Restore-Tests.
- Updates und Wartung der Systeme nach technischem Bedarf.

12. Wiederherstellbarkeit

Ziel:
Sicherstellung, dass personenbezogene Daten nach einem technischen oder physischen Zwischenfall

wiederhergestellt werden können.

Maßnahmen:

- Tägliche Backups.
- Backup-Verwaltung über Backrest.
- Verschlüsselte restic-Repositories.
- Backup-Speicherung bei Hetzner innerhalb der EU.
- Aufbewahrung der Backups derzeit bis zu 3 Monate.
- Regelmäßige Restore-Tests.
- Wiederherstellung aus Backups bei Systemausfall, Datenverlust oder Sicherheitsvorfällen.
- Zugriff auf Backup- und Restore-Funktionen nur für berechtigte Administratoren.

13. Datenschutzfreundliche Voreinstellungen

Ziel:
Datenschutzfreundliche Standardkonfiguration der Anwendung und Prozesse.

Maßnahmen:

- Mandantenbezogene Datenverarbeitung.
- Rollenbasiertes Berechtigungskonzept.
- Benutzer erhalten nur die für ihre Rolle vorgesehenen Funktionen.
- Deaktivierte Benutzerkonten können vom Zugriff ausgeschlossen werden.
- Keine nicht notwendigen Tracking- oder Marketing-Cookies vorgesehen.
- Keine Webanalyse zu Marketingzwecken vorgesehen.
- Keine Drittlandübermittlung vorgesehen.
- Exportfunktionen für Mandantendaten.
- Lösch- und Exportprozesse nach Maßgabe des AVV und Hauptvertrags.
- Supportzugriff nur zweckgebunden und soweit erforderlich.

14. Protokollierung und Monitoring

Ziel:
Erkennung und Nachvollziehbarkeit sicherheitsrelevanter Ereignisse.

Maßnahmen:

- Protokollierung technischer Ereignisse durch Server- und Anwendungskomponenten.
- Systemlog für technische und organisatorische Ereignisse.
- Auditlog für fachliche Änderungen, soweit umgesetzt.
- Security-Logs für sicherheitsrelevante Ereignisse, soweit umgesetzt.
- Login- und Authentifizierungsereignisse können protokolliert werden.
- Protokolle werden zur Fehleranalyse, Sicherheit und Nachweisführung verwendet.
- Zugriff auf Logdaten ist auf berechtigte Personen beschränkt.

15. Umgang mit Datenschutzverletzungen

Ziel:
Schnelle Reaktion auf Sicherheitsvorfälle und Datenschutzverletzungen.

Maßnahmen:

- Sicherheitsvorfälle werden bewertet und dokumentiert.
- Der Verantwortliche wird bei Datenschutzverletzungen, die seine Daten betreffen, unverzüglich informiert.
- Die Information erfolgt möglichst innerhalb von 48 Stunden nach Bekanntwerden.
- Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Bewertung und Erfüllung gesetzlicher Meldepflichten.
- Technische und organisatorische Maßnahmen zur Eindämmung und Behebung von Vorfällen werden ergriffen.
- Protokolldaten können zur Analyse von Sicherheitsvorfällen herangezogen werden.

16. Löschung und Datenexport

Ziel:
Sicherstellung ordnungsgemäßer Löschung und Herausgabe von Daten nach Vertragsende.

Maßnahmen:

- Mandantendaten können über Exportfunktionen exportiert werden.
- Nach Vertragsende besteht eine Exportmöglichkeit für 30 Tage.
- Nach Ablauf der Exportfrist können Kundendaten gelöscht werden, sofern keine gesetzlichen Aufbewahrungspflichten oder berechtigten Gründe entgegenstehen.
- Daten in Backups werden nach Ablauf der Backup-Aufbewahrungsdauer gelöscht oder überschrieben.
- Eine gezielte Einzellöschung aus bestehenden Backup-Ständen ist technisch nur eingeschränkt möglich.
- Backups werden spätestens im Rahmen der regulären Backup-Zyklen überschrieben oder gelöscht.

17. Unterauftragnehmer

Ziel:
Sicherstellung eines angemessenen Datenschutzniveaus bei eingesetzten Dienstleistern.

Unterauftragnehmer	Zweck	Land	Maßnahmen
STRATO	Hosting und technische Bereitstellung der Server-/Web-Infrastruktur.	Deutschland	AV-Vertrag mit STRATO wird abgeschlossen bzw. dokumentiert. Verarbeitung erfolgt im Rahmen der Hosting-Leistung.
Hetzner Online GmbH	Infrastruktur für eigenen Mailserver und Backup-	Deutschland / EU	AV-Vertrag mit Hetzner wird abgeschlossen bzw.

	Speicher.		dokumentiert. Backup-Daten werden verschlüsselt gespeichert. Backup-Übertragung erfolgt über verschlüsselte Verbindung.

18. Regelmäßige Überprüfung

Ziel:
Sicherstellung, dass technische und organisatorische Maßnahmen aktuell und angemessen bleiben.

Maßnahmen:

- TOMs werden bei technischen, organisatorischen oder rechtlichen Änderungen überprüft.
- Sicherheits- und Backup-Prozesse werden bei Bedarf angepasst.
- Restore-Tests werden regelmäßig durchgeführt.
- Änderungen an Infrastruktur, Unterauftragnehmern oder Sicherheitsmaßnahmen werden dokumentiert.
- Diese TOM-Anlage kann bei Weiterentwicklung der Datenschutz-Cloud aktualisiert werden.

19. Hinweise zur Weiterentwicklung

Diese TOM-Anlage beschreibt den aktuellen Stand der technischen und organisatorischen Maßnahmen.

Der Auftragsverarbeiter ist berechtigt, Maßnahmen technisch und organisatorisch weiterzuentwickeln, sofern das Schutzniveau nicht wesentlich unterschritten wird.

Künftige Erweiterungen können insbesondere betreffen:

- weitergehende Protokollierung von Supportzugriffen
- Freigabeprozess für Supportzugriffe durch Mandanten-Admins
- zusätzliche Monitoring- und Alarmierungsmechanismen
- detailliertere Backup- und Restore-Dokumentation
- regelmäßige dokumentierte Sicherheitsüberprüfungen
- zusätzliche Härtungsmaßnahmen auf Server- und Anwendungsebene