

Stand: Oktober 2026 · Version 1.0

Technische und organisatorische Maßnahmen (TOM)

Anlage zum Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO

1. Zweck und Geltungsbereich

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die Strobl & Schmidke Elektrotechnik GmbH (im Folgenden „Anbieter“) als Auftragsverarbeiter beim Betrieb von SUSET ZEIT trifft. Sie konkretisiert Ziff. 9 des Auftragsverarbeitungsvertrags (suset-zeit.de/avv).

Sie gilt für alle Kundeninstanzen von SUSET ZEIT sowie für die zentrale Betriebsverwaltung des Anbieters.

Bei Widersprüchen gilt der AVV.

Die Maßnahmen werden dem technischen Fortschritt angepasst. Änderungen dürfen das hier beschriebene Schutzniveau nicht unterschreiten (AVV Ziff. 9).

2. Systemübersicht

SUSET ZEIT wird als gemanagter Cloud-Dienst betrieben. Die wesentlichen Bestandteile:

BESTANDTEIL	BESCHREIBUNG	STANDORT
Kundeninstanz	Eigene, isolierte Instanz je Kunde mit eigener Datenbank, eigenem Dateispeicher und eigenen Schlüsseln	Deutschland
Server	Hetzner Online GmbH und Hostinger International Ltd.	Deutschland
Externe Sicherung	Hetzner Storage Box (Hetzner Online GmbH)	Deutschland
Zentrale Betriebsverwaltung	Überwachung der Instanzen auf eigenen, gemieteten Servern bei Hetzner bzw. Hostinger in Deutschland. Übermittelt werden nur technische Kennzahlen (z. B. Version, Sicherungsstatus, Speicherbelegung, Fehlerzähler) sowie Firmenname und Lizenzangaben, keine Daten der Beschäftigten.	Deutschland

Der Anbieter betreibt keine Server und lagert keine Datenträger mit Kundendaten in eigenen Büroräumen. Demo-, Test- und Produktivsysteme sind voneinander getrennt; Tests erfolgen ausschließlich mit Testdaten.

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

3.1 Zutrittskontrolle

- Betrieb ausschließlich in professionellen Rechenzentren der Hoster Hetzner Online GmbH und Hostinger International Ltd. in Deutschland; die physische Sicherung (u. a. Zutrittskontrolle) richtet sich nach den technischen und organisatorischen Maßnahmen der Rechenzentrumsbetreiber.
- Keine Server oder Datenträger mit Kundendaten in Büroräumen des Anbieters.

3.2 Zugangskontrolle — Server und Betrieb

- Anmeldung an den Servern nur per SSH mit Schlüssel (keine Passwort-Anmeldung) und nur über ein abgesichertes VPN.
- Notfallzugang ausschließlich über die Web-Konsole des Hosters; die Hoster-Konten sind mit einem langen Passwort und Zwei-Faktor-Authentifizierung geschützt.

- Firewall: Von außen erreichbar sind nur HTTP/HTTPS sowie einzeln freigegebene Dienst-Ports.
- Vor dem Webserver arbeitet CrowdSec mit Community-Sperrlisten zur Abwehr von Angriffen. Dabei werden IP-Adressen erkannter Angreifer mit der CrowdSec-Community (CrowdSec SAS, Frankreich) ausgetauscht.
- Zugangsdaten und Geheimnisse des Betriebs werden in einem Passwortmanager verwaltet.
- Die zentrale Betriebsverwaltung ist nur mit Passwort, Zwei-Faktor-Authentifizierung und einem zusätzlich vorgeschalteten HTTP-Zugangsschutz erreichbar. Jede Instanz verwendet für die Übermittlung an die Betriebsverwaltung einen eigenen, langen Zugriffsschlüssel. Übermittelt werden nur technische Kennzahlen (z. B. Version, Sicherungsstatus, Speicherbelegung, Fehlerzähler) sowie Firmenname und Lizenzangaben, keine Daten der Beschäftigten.
- Die zentrale Betriebsverwaltung läuft auf eigenen, gemieteten Servern bei Hetzner bzw. Hostinger in Deutschland, getrennt von den Kundeninstanzen.

3.3 Zugangskontrolle — Anwendung

- Passwörter werden ausschließlich als bcrypt-Hash gespeichert.
- Passwort-Richtlinie: Mindestlänge und Komplexität einstellbar, Abgleich mit verbreiteten Passwörtern, der eigene Name ist nicht zulässig; keine erzwungene regelmäßige Änderung (entsprechend der Empfehlung des BSI).
- Zwei-Faktor-Authentifizierung (TOTP): für Administratoren immer Pflicht, für Mitarbeiter einschaltbar; Wiederherstellungscodes für den Verlust des zweiten Faktors.
- Optional „Gerät merken“: Auf einem vertrauenswürdigen Gerät entfällt der Zwei-Faktor-Code für 30 Tage; das Passwort bleibt immer Pflicht. Die Markierung ist signiert, lässt sich im Profil jederzeit widerrufen und wird beim Zurücksetzen oder Abschalten der Zwei-Faktor-Anmeldung ungültig.
- Sperre nach Fehlversuchen: IP-Adresse nach 5, Benutzerkonto nach 10 fehlgeschlagenen Anmeldungen, jeweils für 15 Minuten.
- Sitzungen enden nach 24 Stunden Inaktivität, spätestens nach 30 Tagen. Nutzer sehen ihre angemeldeten Geräte und können sie aus der Ferne abmelden.
- Passwort-Zurücksetzen nur über einmalige, befristete Links; in der Datenbank wird nur ein Hash gespeichert.
- Stempeluhr-Tablets müssen vor der Nutzung gekoppelt werden; PINs und NFC-Kennungen werden nur als Hash gespeichert.

3.4 Zugriffskontrolle

- Rollenkonzept: Mitarbeiter, frei definierbare Zwischenrollen und Administrator. Mitarbeiter sehen ausschließlich ihre eigenen Daten.
- Vor besonders sensiblen Aktionen ist eine erneute Passwortbestätigung erforderlich: Wiederherstellen und Herunterladen von Sicherungen, Zurücksetzen der Zwei-Faktor-Authentifizierung, Erzeugen von API-Schlüsseln.
- Hochgeladene Dateien sind nur für die betroffene Person und berechtigte Administratoren abrufbar.
- Der Anbieter hat kein eigenes Benutzerkonto in den Kundeninstanzen. Ein Zugriff auf Inhalte ist nur direkt über den Server möglich und erfolgt nur für Betrieb, Fehlerbehebung, Support oder auf Bitte des Kunden (AVV Ziff. 2).
- An die zentrale Betriebsverwaltung werden nur technische Kennzahlen (z. B. Version, Sicherungsstatus, Speicherbelegung, Fehlerzähler) sowie Firmenname und Lizenzangaben, keine Daten der Beschäftigten (siehe Ziff. 3.2).

3.5 Trennungskontrolle

- Jeder Kunde erhält eine eigene, isolierte Instanz mit eigener Datenbank, eigenem Dateispeicher und eigenen Schlüsseln.
- Demo-, Test- und Produktivsysteme sind getrennt; Tests erfolgen ausschließlich mit Testdaten.

3.6 Verschlüsselung

- Alle Verbindungen sind per TLS (HTTPS) verschlüsselt.
- Verschlüsselt gespeichert (AES-256-GCM) werden: Geheimnisse der Zwei-Faktor-Authentifizierung, Zugangsdaten für E-Mail-Dienste und Schlüssel für Push-Benachrichtigungen.
- Sicherungen können optional kennwortverschlüsselt heruntergeladen werden (AES-256-GCM).
- Die Datenträger der Cloud-Server sind nicht zusätzlich verschlüsselt. Ihr Schutz richtet sich nach den technischen und organisatorischen Maßnahmen der Rechenzentrumsbetreiber.

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

4.1 Weitergabekontrolle

- Übertragungen erfolgen ausschließlich verschlüsselt (TLS).
- Schnittstellen zu anderen Systemen sind erst nach Aktivierung durch den Kunden nutzbar. Eingehende Aufrufe erfordern einen API-Schlüssel, ausgehende Meldungen sind mit HMAC signiert, Anfragen werden begrenzt.
- Sensible Dokumente (z. B. Lohnabrechnungen) werden per E-Mail nur als Link versendet, nicht als Anhang. Downloads sensibler Dateien werden protokolliert.

4.2 Eingabekontrolle

- Unveränderliches Protokoll relevanter Vorgänge; die Einträge sind über eine SHA-256-Hash-Kette verknüpft, die automatisch auf Veränderungen geprüft wird.
- Datenbank-Schutzregeln verhindern das Ändern und Löschen von Protokolleinträgen.
- Änderungshistorie je Zeiteintrag mit Begründung; Korrekturbuchungen werden storniert statt gelöscht.
- Archivierte Monatsberichte erhalten eine Prüfsumme.

4.3 Schutz vor Schadinhalten

- Hochgeladene Dateien werden anhand ihres tatsächlichen Inhalts geprüft, nicht anhand der Dateiendung.
- Aus PDF-Dateien werden Skripte, eingebettete Dateien und Formularaktionen entfernt; Bilder werden neu erzeugt.
- Content-Security-Policy mit Einmalwert gegen eingeschleuste Skripte.

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

- Überwachung der Datenbank mit automatischem Neustart.
- Integritätsprüfung von Datenbank und Protokoll zweimal täglich; tägliche inhaltliche Selbstprüfung der Daten.
- Erkennung, wenn eine Instanz auf einen älteren Datenstand zurückspringt.
- Fehler und Sicherheitsereignisse werden den Administratoren der Instanz gemeldet.
- Abwehr von Angriffen durch Firewall, CrowdSec (Ziff. 3.2), Anmeldesperren (Ziff. 3.3) und Anfragebegrenzung für Schnittstellen (Ziff. 4.1).

6. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Tägliche automatische Sicherung jeder Instanz (Datenbank und Dateien), signiert mit HMAC-SHA256, mit gestaffelter Aufbewahrung. Die Sicherung ist nicht abschaltbar.
- Zusätzliche automatische Sicherung vor jedem Update und vor jeder Wiederherstellung.

- Externe Sicherung der Server auf einer Hetzner Storage Box in Deutschland mit gestaffelter Aufbewahrung (täglich, wöchentlich, monatlich; höchstens 12 Monate).
- Täglicher automatischer Wiederherstellungstest der neuesten Sicherung (Signatur, Vollständigkeit, Datenbankintegrität).
- Vor einer Wiederherstellung werden Signatur und Integrität geprüft. Die Anwendung zeigt an, welche Daten seit dem Sicherungsstand verloren gingen; die Wiederherstellung erfordert eine ausdrückliche Bestätigung.

7. Organisatorische Maßnahmen

7.1 Personal

- Zugriff auf Systeme mit Kundendaten haben derzeit ausschließlich die Geschäftsführer des Anbieters.
- Künftige Beschäftigte mit Zugriff werden vorher schriftlich auf Vertraulichkeit verpflichtet und unterwiesen, erhalten personenbezogene Zugänge, und ihre Zugänge werden beim Ausscheiden entzogen.

7.2 Verletzungen des Schutzes personenbezogener Daten

- Vorfälle werden unverzüglich eingedämmt und bewertet.
- Der Kunde wird unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, in Textform informiert — mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.
- Vorfälle werden dokumentiert.

7.3 Updates und Schwachstellen

- Jede neue Version wird vor der Auslieferung automatisiert geprüft: Typprüfung, Code-Prüfung, Unit- und Browser-Tests sowie Prüfung der verwendeten Bibliotheken auf bekannte Sicherheitslücken. Ausgerollt wird erst nach bestandener Prüfung.
- Sicherheitsupdates für Betriebssystem, Server-Software und Bibliotheken werden zeitnah nach Bekanntwerden eingespielt; die Systeme werden regelmäßig aktualisiert.
- Die verwendeten Bibliotheken werden wöchentlich automatisch auf Updates und bekannte Sicherheitslücken geprüft.

7.4 Auftragskontrolle

- Unterauftragsverarbeiter werden nur gemäß AVV Ziff. 10 eingesetzt und vertraglich nach Art. 28 Abs. 4 DSGVO verpflichtet.
- Zugriffe des Anbieters auf Inhalte der Kundeninstanzen erfolgen nur im Rahmen von AVV Ziff. 2 (siehe Ziff. 3.4).

7.5 Löschung

- Bei Vertragsende wird die gesamte Kundeninstanz gelöscht — einschließlich Datenbank, Dateien und der darin enthaltenen Sicherungen (Fristen gemäß AVV Ziff. 13).
- Externe Sicherungen werden im Rahmen der regulären Rotation spätestens 13 Monate nach Vertragsende gelöscht.
- Die Löschung wird auf Anfrage in Textform bestätigt.

8. Regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Die Maßnahmen werden bei wesentlichen Änderungen, mindestens jedoch jährlich überprüft und bei Bedarf angepasst.

- Laufende automatisierte Prüfungen ergänzen die Überprüfung: täglicher Wiederherstellungstest (Ziff. 6), Integritätsprüfungen (Ziff. 5), Prüfung jeder Version und wöchentliche Prüfung der Bibliotheken (Ziff. 7.3).

9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Standorterfassung, Push-Benachrichtigungen, Schnittstellen und E-Mail-Versand sind standardmäßig ausgeschaltet. Standortdaten werden nur nach Aktivierung durch den Kunden und Freigabe im Browser des Nutzers erfasst.
- Jeder Nutzer kann seine gespeicherten Daten als Datei herunterladen (Auskunft und Datenübertragbarkeit nach Art. 15 und 20 DSGVO).
- Ausgeschiedene Mitarbeiter können endgültig gelöscht werden; Daten mit gesetzlichen Aufbewahrungspflichten bleiben dabei erhalten.
- Die Funktion „Ansicht als Mitarbeiter“ für Administratoren ist nur lesend und wird protokolliert.
- Fehlerprotokolle enthalten keine E-Mail-Adressen, IP-Adressen oder Schlüssel und werden nach 30 Tagen gelöscht.

Stand: Oktober 2026 · Version 1.0