Technische und organisatorische Maßnahmen (TOMs)

Stand: 2026-05-09

1. Zweck

Diese technischen und organisatorischen Maßnahmen beschreiben die Vorkehrungen zum Schutz personenbezogener Daten, die im Rahmen von SDS Engine verarbeitet werden. Ziel ist es, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten angemessen sicherzustellen.

2. Zutrittskontrolle

- Relevante Systeme werden bei spezialisierten Infrastruktur- und Hosting-Anbietern betrieben.

- Der physische Zugang zu Rechenzentren wird durch die jeweiligen Infrastrukturbetreiber kontrolliert und beschränkt.

- Der Anbieter selbst unterhält keine ungesicherten Serverstandorte mit direktem Publikumszugang für produktive Kundendaten.

3. Zugangskontrolle

- Der Zugriff auf administrative Systeme und Produktivumgebungen erfolgt nur für berechtigte Personen.

- Zugänge zu Produktivsystemen werden über individuelle Konten verwaltet.

- Es werden starke Authentifizierungsmechanismen und passwortgeschützte Zugänge verwendet.

- Nicht mehr benötigte Zugänge werden deaktiviert oder entfernt.

4. Zugriffskontrolle und Berechtigungskonzept

- Der Zugriff auf Daten innerhalb der Anwendung erfolgt rollen- und berechtigungsbasiert.

- Nutzer sehen grundsätzlich nur Daten ihres eigenen Unternehmensmandanten.

- Administrative Sonderrechte werden nur im erforderlichen Umfang vergeben.

- Änderungen an Rollen, Berechtigungen und sensiblen Einstellungen werden protokolliert oder nachvollziehbar verarbeitet, soweit technisch vorgesehen.

5. Mandantentrennung

- Kundendaten werden logisch mandantengetrennt verarbeitet.

- Zugriffe auf Unternehmensdaten werden in der Anwendung anhand von Organisationszuordnungen und Berechtigungen eingeschränkt.

- Öffentliche oder vereinfachte Zugriffswege, etwa QR-basierte Ansichten, werden nur für ausdrücklich dafür vorgesehene Inhalte bereitgestellt.

6. Weitergabekontrolle und Übertragungssicherheit

- Die Datenübertragung zwischen Endgeräten und der Plattform erfolgt verschlüsselt über aktuelle Transportverschlüsselung.

- Externe Dienste werden nur im Rahmen der vereinbarten oder technisch erforderlichen Verarbeitung eingebunden.

- Öffentliche Links werden, soweit technisch vorgesehen, mit nicht erratbaren Tokens erzeugt und können bei Bedarf neu generiert werden.

7. Eingabekontrolle und Nachvollziehbarkeit

- Relevante Vorgänge innerhalb der Plattform können über Aktivitäts- und Systemprotokolle nachvollzogen werden.

- Protokolliert werden können insbesondere Logins, Uploads, Änderungen an Stoffdaten, Prüfaktionen, Zuordnungen sowie abrechnungsbezogene Vorgänge.

- Audit- und Sicherheitslogs können auch dann erhalten bleiben, wenn produktive Kundendaten gelöscht oder anonymisiert werden, soweit dies rechtlich zulässig ist.

8. Verfügbarkeitskontrolle

- Es bestehen Maßnahmen zur Überwachung und Stabilisierung des Produktivbetriebs.

- Daten werden bei eingesetzten Infrastruktur- und Plattformdiensten redundant oder in den dort vorgesehenen Schutzmechanismen gespeichert, soweit dies vom jeweiligen Dienst unterstützt wird.

- Für den Ausfall von Teilsystemen bestehen technische und organisatorische Verfahren zur Fehleranalyse und Wiederherstellung im angemessenen Rahmen.

9. Integrität und Belastbarkeit

- Systeme und Komponenten werden laufend weiterentwickelt und technisch gepflegt.

- Sicherheitsrelevante Anpassungen, Fehlerbehebungen und technische Änderungen können eingespielt werden, um den sicheren und stabilen Betrieb aufrechtzuerhalten.

- Der Anbieter bemüht sich um eine angemessene Belastbarkeit der verarbeiteten Systeme, ohne eine vollständig unterbrechungsfreie Verfügbarkeit zu garantieren.

10. Trennbarkeit unterschiedlicher Verarbeitungszwecke

- Daten werden nur in dem Umfang verarbeitet, wie dies zur Vertragserfüllung, zur Systemsicherheit, zur Abrechnung, zur Fehlerbehebung oder zur Erfüllung gesetzlicher Pflichten erforderlich ist.

- Produktive Kundendaten, Supportinformationen, Sicherheitsprotokolle und abrechnungsbezogene Informationen werden nach Möglichkeit zweckgebunden verarbeitet.

11. Löschung und Anonymisierung

- Personenbezogene Daten werden nach Vertragsende oder auf berechtigte Weisung gelöscht oder anonymisiert, soweit keine gesetzlichen Aufbewahrungspflichten oder berechtigten Interessen entgegenstehen.

- Eine Löschung produktiver Kundendaten kann nicht in jedem Fall rückgängig gemacht werden.

- Einzelne Sicherheits-, Nachweis- oder Abrechnungsprotokolle können im rechtlich zulässigen Umfang weiter gespeichert werden.

12. Unterauftragsverarbeiter und Drittanbieter

- Für den Betrieb von SDS Engine können spezialisierte Unterauftragsverarbeiter und Infrastrukturdienstleister eingesetzt werden.

- Mit relevanten Auftragsverarbeitern werden geeignete vertragliche Datenschutzregelungen abgeschlossen oder deren bereitgestellte Standard-DPA genutzt, soweit dies datenschutzrechtlich erforderlich ist.

- Änderungen im Kreis relevanter Unterauftragsverarbeiter werden nach Maßgabe der AVV behandelt.

13. Vorfallsmanagement

- Sicherheitsrelevante Vorfälle werden intern geprüft und dokumentiert, soweit dies technisch und organisatorisch vorgesehen ist.

- Soweit personenbezogene Daten des Verantwortlichen betroffen sind, erfolgt eine Information nach Maßgabe der AVV und der gesetzlichen Vorgaben.

- Der Anbieter trifft im Rahmen seiner Möglichkeiten angemessene Maßnahmen zur Eindämmung, Analyse und Behebung sicherheitsrelevanter Vorfälle.

14. Überprüfung und Weiterentwicklung

- Die technischen und organisatorischen Maßnahmen werden bei Bedarf überprüft und fortentwickelt.

- Der Anbieter ist berechtigt, bestehende Maßnahmen zu ändern, sofern das datenschutzrechtlich erforderliche Schutzniveau nicht unterschritten wird.