SCOPEVISIO

Anhang I – AVV nach Art. 28 DSGVO
für die SaaS-Anwendung „SVFN Cloud“

Technisch-organisatorische Maßnahmen zur Einhaltung des Datenschutzes

Stand: 26. August 2026

1 Einleitung

Die nachfolgendend beschriebenen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO beschreiben die von der

Scopevisio AG, Konrad-Zuse-Platz 7, 53227 Bonn

umgesetzten Schutzmaßnahmen für die Verarbeitung personenbezogener Daten für die SaaS-Anwendung „SVFN Cloud“.

2 Rechenzentrum

Die Datenverarbeitung bei der Nutzung von SVFN Cloud erfolgt in einem Rechenzentrum, das von einem Dienstleister der Scopevisio AG betrieben wird. Die von den Betreibern getroffenen physischen und infrastrukturellen Sicherheitsmaßnahmen ergänzen die nachfolgend beschriebenen eigenen Maßnahmen von der Scopevisio AG.

- Rechenzentrumsbetreiber:
  - **mitteldeutsche IT GmbH**
    Debyestraße 5b, 04329 Leipzig, Deutschland

- Zertifizierungen und Testate:
  - C5-Testat des BSI
    (Cloud Computing Compliance Criteria Catalogue)
  - ISO/IEC 27001:2022

3 Vertraulichkeit

3.1 Zutrittskontrolle

Maßnahmen zum Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen.

Hinweis: Die physische Sicherheit der Rechenzentren wird durch den Betreiber (mitteldeutsche IT GmbH) gewährleistet. Die folgenden Maßnahmen beziehen sich auf die eigenen Standorte der Scopevisio AG.

Technische Maßnahmen

- ☑ Räumliche Begrenzung des Betriebsgeländes
- ☑ Sicherheitsschlösser
- ☑ Manuelles Schließsystem mit Codesperren
- ☑ Spezielles Schließsystem für verschlossene Bereiche
- ☑ Zutrittskontrollsystem mit Transponder
- ☑ Videoüberwachung

Organisatorische Maßnahmen

- ☑ Besucheranmeldung
- ☑ Sorgfältige Auswahl von Reinigungs- und Wachpersonal
- ☑ Schlüsselregelung mit dokumentierter Schlüsselausgabe

3.2 Zugangskontrolle

Maßnahmen zur Sicherstellung, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten.

Technische Maßnahmen

- ☑ Benutzeranmeldung mit individueller Kennung und Passwort
- ☑ Zwei-Faktor-Authentifizierung
- ☑ Software-Firewalls auf Servern und Clients
- ☑ Firewall-Konfiguration nach Whitelist-Prinzip (nur explizit erlaubter Datenverkehr)
- ☑ VPN-Tunnel für den Remote-Zugriffe
- ☑ Einsatz eines Endpoint-Detection-and-Response-Systems (EDR)
- ☑ Authentifizierung mittels biometrischer Daten
- ☑ Sperrung von Clients bei Inaktivität

Organisatorische Maßnahmen

- ☑ Benutzerberechtigungsmanagement nach dem Least-Privilege- und Need-to-Know-Prinzip
- ☑ Benutzer- und Rollenprofile
- ☑ Passwortrichtlinie (Komplexität, Änderungsintervalle, Geheimhaltung)
- ☑ Verpflichtung der Mitarbeiter auf Vertraulichkeit
- ☑ Richtlinie zum zulässigen Gebrauch / Acceptable Use Policy (AUP)
- ☑ Dokumentation von Berechtigungen
- ☑ Anlassbezogene Aktualisierung von Berechtigungen (z. B. bei Abteilungswechsel oder Austritt)
- ☑ Regelmäßige Überprüfung der vergebenen Berechtigungen
- ☑ Sichere Aufbewahrung von Datenträgern

3.3 Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben (Lesen, Kopieren, Verändern oder Entfernen innhalb des Systems).

Technische Maßnahmen

- ☑ Sichere Vernichtung von Datenträgern
- ☑ Protokollierung der Vernichtung von Daten
- ☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten
- ☑ Verschlüsselung von Datenträgern und mobilen Endgeräten (Festplattenverschlüsselung)
- ☑ Identifizierungs- und Authentifizierungssystem

Organisatorische Maßnahmen

- ☑ Vergabe von Zugriffsrechten nach dem Least-Privilege-Prinzip
- ☑ Einsatz von Dienstleistern zur Akten- und Datenvernichtung
- ☑ Passwortmanagement
- ☑ Dokumentiertes Verfahren zur Rechteverwaltung (Rechtemanagement)
- ☑ Vier-Augen-Prinzip bei Spezialanwendungen (Fernwartung, Protokollauswertung u. a.)
- ☑ Vergabe von Berechtigungen nach dem Need-to-Know-Prinzip

3.4 Trennungskontrolle

Maßnahmen zur Sicherstellung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

Technische Maßnahmen

- ☑ Anonymisierung von Datensätzen und anschließend getrennte Verarbeitung (z. B. in Analysesystemen)
- ☑ Trennung von Produktiv- und Testsystemen
- ☑ Logische Mandantentrennung (softwareseitig)

Organisatorische Maßnahmen

- ☑ Erstellung und Pflege eines Berechtigungskonzepts
- ☑ Festlegung von Datenbankrechten
- ☑ Mitarbeiterschulung zur Zweckbindung und getrennten Verarbeitung von personenbezogenen Daten

3.5 Pseudonymisierung

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen

- ☑ Automatische Verschlüsselung von Datensätzen
- ☑ Gesonderte Ablage des Entschlüsselungsschlüssels mit eigener Zugriffsberechtigung

Organisatorische Maßnahmen

- ☑ Manuelle Kürzung von Datensätzen
- ☑ Manuelle Überschreibung von Datensätzen einschließlich dokumentiertem Wiederherstellungsprozess mit Berechtigungsfreigabe
- ☑ Mitarbeiterschulung zur korrekten Anwendung von Pseudonymisierungsverfahren

4 Integrität, Verfügbarkeit und Belastbarkeit

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

4.1 Weitergabekontrolle

Maßnahmen zur Sicherstellung, dass personenbezogene Daten bei der elektronischen Übertragung oder beim Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- ☑ Verschlüsselung von Laptops mit Zugangssicherung durch Benutzerkonto und Passwort
- ☑ Inhaltsverschlüsselung nach Bedarf, sofern erforderlich
- ☑ Transportverschlüsselung (TLS/SSL)
- ☑ Elektronische Signatur
- ☑ Einsatz von E-Mail-Content-Filtern
- ☑ Sichere VPN-Technologie

Organisatorische Maßnahmen

- ☑ Logfiles zur Dokumentation und Überprüfung der Serverzugriffe
- ☑ Berechtigungskonzept
- ☑ Vernichtung von Papierakten und -unterlagen durch externe Dienstleister gegen Bestätigung
- ☑ Sichere Löschung und Vernichtung von Datenträgern durch mechanische Zerstörung

4.2 Eingabekontrolle

Maßnahmen zur Sicherstellung, dass nachvollzogen werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen

- ☑ Protokollierung der Eingabe, Änderung und Löschung von Daten (Userdatenbank)
- ☑ Nachvollziehbarkeit von Datenänderungen durch individuelle Benutzernamen (nicht Benutzergruppen)

Organisatorische Maßnahmen

- ☑ Digitales Berechtigungskonzept
- ☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines dokumentierten Berechtigungskonzepts

4.3 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Maßnahmen zum Schutz personenbezogener Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust sowie zur raschen Wiederherstellung der Verfügbarkeit nach einem Zwischenfall.

Hinweis: Infrastrukturelle Verfügbarkeitsmaßnahmen (USV, Klimatisierung, Brandschutz) werden in den Rechenzentren durch die jeweiligen Betreiber sichergestellt und sind durch deren Zertifizierungen nachgewiesen.

Technische Maßnahmen

- ☑ Regelmäßige Datensicherungen (Backup-Verfahren)
- ☑ Firewall und Intrusion-Detection-System (IDS)
- ☑ Feuer- und Rauchmelder in den eigenen Büroräumen
- ☑ Klimatisierung von Serverräumen
- ☑ USV (Unterbrechungsfreie Stromversorgung)
- ☑ Load-Balancing

Organisatorische Maßnahmen

- ☑ Backup- und Recovery-Konzept
- ☑ Notfallplan und Notfallmanagement
- ☑ Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- ☑ Festlegung von Meldewegen bei Sicherheitsvorfällen
- ☑ Regelmäßige Tests zur Datenwiederherstellung
- ☑ Feuerlöscher in den eigenen Büroräumen

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1 Datenschutz-Management

Technische Maßnahmen

- ☑ Regelmäßige Penetrationstests
- ☑ Incident-Response-Management

Organisatorische Maßnahmen

- ☑ Bestellung eines Datenschutzbeauftragten
- ☑ Regelmäßiges Berichtswesen an die Geschäftsführung
- ☑ Informations- und IT-Sicherheitskonzept
- ☑ Datenschutzkonzept
- ☑ Regelmäßige interne Überprüfung und Aktualisierung der getroffenen Maßnahmen gemäß dem Stand der Technik (durch DSB, IT-Revision o. Ä.)

5.2 Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung

Technische Maßnahmen

- ☑ Verwendung von Opt-in-Lösungen
- ☑ Minimierung von Pflichtfeldern bei Registrierungen
- ☑ Deutliche Kennzeichnung von freiwilligen Angaben
- ☑ Beschränkung der erhobenen Daten und deren Weiterverwendung auf das notwendige Maß
- ☑ Automatisierte Löschfunktionen für Logfiles

Organisatorische Maßnahmen

- ☑ Transparente Datenverarbeitung (Funktionsbeschreibung, Überwachungsmöglichkeit durch Betroffene)
- ☑ Regelungen zur Datenminimierung, Datensparsamkeit und Erforderlichkeit
- ☑ Beschränkung der Speicherfrist

6 Auftragskontrolle

(Art. 28 DSGVO)

Maßnahmen zur Sicherstellung, dass personenbezogene Daten im Rahmen einer Auftragsverarbeitung nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

Technische Maßnahmen

- ☑ Überprüfung aller vertraglich zugesicherten technischen Maßnahmen, z. B. durch Vorlage von Zertifizierungen und Prüfberichten

Organisatorische Maßnahmen

- ☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☑ Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen mit entsprechender Dokumentation und Nachweisen
- ☑ Regelmäßige Überprüfung des Auftragnehmers hinsichtlich Datenschutz und Datensicherheit
- ☑ Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Art. 28 DSGVO
- ☑ Vereinbarung von wirksamen Kontrollrechten gegenüber dem Auftragnehmer
- ☑ Mitarbeiterschulung zum Umgang mit personenbezogenen Daten