Technische und organisatorische Maßnahmen (TOMs)

avs SYSTEM LIFT AG
Hannoversche Straße 115 a
30916 Isernhagen

Stand Januar 2026

Inhaltsverzeichnis

A. Dokumenthistorie

Datum	Autor	Beschreibung
18.12.2017	Malte Bilau Marco Kinscher	Erste Version.
19.02.2018	Malte Bilau	Überarbeitung und Ergänzung durch TOMs des Rechenzentrums.
25.04.2023	Malte Bilau Adrian Tamm	Aktualisierung durch Umzug nach Isernhagen.
12.12.2025	Adrian Tamm Sascha Kahrels	Aktualisierung unter Berücksichtigung des neuen Schulungsportals.

B. Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) schreibt gemäß Art. 32 vor, dass Unternehmen für die Sicherheit von Daten zu sorgen haben. Die hierfür umzusetzenden technischen und organisatorischen Maßnahmen (TOMs) sollen dabei geeignet sein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung von Daten auf Dauer sicherzustellen. Dabei sind die Art und der Umfang der Datenverarbeitung genauso zu berücksichtigen, wie der Stand der Technik sowie die Implementierungskosten.

Dieses Dokument beschreibt die umgesetzten TOMs. Dabei unterliegen die TOMs dem technischen Fortschritt, sodass die beschriebenen Maßnahmen kontinuierlich überprüft und ggf. angepasst werden. Die Änderungen sind in diesem Dokument jeweils zeitnah anzupassen.

C. Vertraulichkeit

C.1 Zutrittskontrolle

Es haben ausschließlich befugte Personen Zutritt den Geschäftsräumen. Alle Eingänge sind von außen nur mittels Schlüssel bzw. Transponder zu öffnen. Die Ausgabe der Schlüssel erfolgt protokolliert.

Besucher müssen klingeln und werden durch Beschäftigte in Empfang genommen. Während Ihres Besuchs werden die Besucher von Beschäftigten begleitet und haben keinen Zugang zu den Büros, sondern lediglich zu allgemeinen Besprechungsräumen.

Die Reinigung der Büroräume erfolgt durch einen externen Dienstleister, mit dem eine Geheimhaltungsvereinbarung abgeschlossen wurde.

Die Eingänge werden videoüberwacht. Es ist eine Alarmanlage installiert. Diese wird außerhalb der Bürozeiten durch den letzten Beschäftigten, der das Büro verlässt, scharf geschaltet. Alarme werden extern signalisiert und an die Vorstände übermittelt.

C.2 Zugangskontrolle

Die Netzwerkverkabelung erfolgt nur innerhalb der abgesicherten Büroräume. Es gibt eine dedizierte Firewall zum Internetzugang. Ein Zugriff von außen auf das interne Netz ist nur mittels verschlüsselter VPN-Verbindungen möglich.

Im Netz identifizieren sich die Benutzer mittels individuelle Benutzernamen und sicheren Passworten. Der Passwortaufbau wird dabei durch technische Vorgaben sicher gestaltet.

Für mobile Geräte gelten ebenso die vorgenannten technischen Restriktionen. Weiterhin werden hier biometrische Verfahren (Face-ID) zur Identifikation verwendet.

Die Arbeitsplatzgeräte und Server werden zusätzlich durch eine Software-Firewall und einen Virenscanner gesichert.

C.3 Zugriffskontrolle

Die Verwaltung aller Benutzerrechte erfolgt durch Systemadministratoren und die Anzahl der Administratoren ist dabei auf ein Minimum reduziert. Die Benutzerrechte werden gemäß eines Berechtigungskonzepts und nach Genehmigung durch die Geschäftsleitung vergeben.

Datenträger werden gesichert aufbewahrt und nach Bedarf datenschutzgerecht gelöscht und entsorgt. Weiterhin wird zur Aktenvernichtung ein externer Dienstleister eingesetzt, durch den die Löschung protokolliert erfolgt.

C.4 Trennungskontrolle

Interne Server und Anwendungen werden vom Schulungsportal getrennt betrieben. Innerhalb des Schulungsportals erfolgt eine Mandantentrennung softwareseitig.

C.5 Pseudonymisierung

Eine durch Pseudonyme geschützte Datenverarbeitung wird überall dort eingesetzt, wo es sinnvoll ist. Die Zuordnung erfolgt dabei über getrennte Datenbanktabellen.

D. Integrität

D.1 Weitergabekontrolle

Digitale Datenübermittlungen erfolgen grundsätzlich über verschlüsselte Verbindungen. Der Zugriff von außen auf die Firmeninfrastruktur ist über eine verschlüsselte VPN-Verbindung möglich. Für Zugriffe per Internet werden die Verbindungen per HTTPS verschlüsselt.

Die E-Mail-Kommunikation erfolgt transportverschlüsselt. Eventuell werden auch Dateianhänge separat verschlüsselt. Der Zugriff auf E-Mails während der Abwesenheit von Beschäftigten ist geregelt.

Für Briefpost gibt es einen Briefkasten nach DIN EN13724. Der Zugriff zur Post ist nur mit entsprechendem Schlüssel möglich. Zugriff haben nur berechtigte Personen.

Auf Systeme des Verantwortlichen wird durch Dienstleister über Fernwartungstools ebenfalls nur über verschlüsselte Verbindungen zugegriffen.

D.2 Eingabekontrolle

Im DATEV Unternehmen online, Microsoft 365 und im Schulungsportal wird das Anlegen, Verändern und Löschen von Daten protokolliert. Über die individuellen Benutzernamen ist nachvollziehbar, wer Anpassungen vorgenommen hat.

Teilweise wird mit Formularen gearbeitet, deren Inhalte in digitale Systeme übernommen werden. Die Originalformulare werden dabei zur Nachvollziehbarkeit von eventuellen Eingabefehlern aufgehoben.

E. Verfügbarkeit und Belastbarkeit

E.1 Verfügbarkeitskontrolle

Um die Verfügbarkeit von Daten zu gewährleisten, werden unterbrechungsfreie Stromversorgungen (USV) und Klimaanlagen in Serverräumen eingesetzt. Weiterhin existieren Feuer- und Rauchmeldeanlagen sowie Feuerlöscher. Alle Server sind oberhalb der Wassergrenze installiert und nicht unterhalb von sanitären Anlagen untergebracht.

Datensicherungen erfolgen gemäß eines Backup-Konzepts regelmäßig, wobei immer mehrere Sicherungen verfügbar gehalten werden.

E.2 Rasche Wiederherstellbarkeit

Die Sicherungen werden regelmäßig geprüft und stichprobenartig wiederhergestellt. So ist im Notfall eine schnelle Wiederinbetriebnahme gewährleistet.

F. Verfahren zur regelmäßigen Überprüfung und Bewertung

F.1 Datenschutzmanagement

Ein externer Datenschutzbeauftragter ist schriftlich benannt. Es existiert eine interne Verarbeitungsübersicht der Verarbeitungsprozesse. Mittels eines Datenschutz-Management-Systems wird eine wiederkehrende Kontrolle alle datenschutzrelevanten Vorgänge gewährleistet.

Die Beschäftigten erhalten jeweils zu Beginn ihrer Tätigkeit und danach regelmäßig Schulungen zum Datenschutz und allgemeine Sensibilisierungen zur IT-Sicherheit. Hierbei kommen sowohl Online-Schulungen als auch Präsenzschulungen zum Einsatz.

Darüber hinaus werden die Beschäftigten auf Vertraulichkeit verpflichtet. Auch diese Verpflichtung wird zu Beginn der Tätigkeit sowie anschließend regelmäßig erneuert.

F.2 Incident-Response-Management

Datenschutzvorfälle werden von der Geschäftsleitung in Zusammenarbeit mit dem externen Datenschutzbeauftragten bearbeitet.

F.3 Auftragskontrolle

Die Auftragsverarbeiter werden hinsichtlich Datensicherheit sorgfältig ausgewählt. Darüber hinaus wird, sofern notwendig, eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Darüber werden sowohl die notwendigen Kontrollrechte definiert als auch und die Datenlöschung bei Auftragsende sichergestellt.

Die Schutzmaßnahmen der Dienstleister werden regelmäßig unter Zuhilfenahme des externen Datenschutzbeauftragten kontrolliert. Diese Kontrolle erfolgt je Einzelfall durch Fragebögen, Überprüfung von Zertifikaten externer Auditoren oder auch eigenen Inspektionen.