

TOM 2026.1

gültig ab 01.01.2026

Änderungshinweise

Initiale digitale Version

Aufgabe und Geltungsbereich

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen zur Wahrung des Datenschutzes von Kunden und firmeninternen Daten im Bereich der Datenverarbeitung in internen Systemen der Firma system-helden sowie im Bereich der Datenverarbeitung im angemieteten Rechenzentrum (Standort Am Spingborn 1, Köln) durch die Firma system-helden. Die ergriffenen Maßnahmen entsprechen dem aktuellen Stand der Technik

Vertraulichkeit 1.

1.1 Zutrittskontrolle

Der Zugang zu sowie der Zugriff auf Datenverarbeitungssysteme sowie Daten von Kunden und Mitarbeitern

wird durch folgende technische Datenschutzmaßnahmen sicher gestellt:

Ort / Objekt	Zugangsschutz	Zugangsregelung
--------------	---------------	-----------------

Serverraum / Lager	biometrische Zugangskontrolle (Fingerabdruck)	Nur Personen mit Berechtigung zum Lagerzugriff sowie Vorgesetzte haben Zugriff auf das Lager, Öffnungen des Lagers werden protokolliert (automatisch, elektronisch). Der Lager und Serverbereich wird Videoüberwacht
Serverschrank	mechanisches Schließsystem	Schlüsselausgabe nur an berechtigte Personen
Zugang Firmengelände	biometrische Zugangskontrolle (Fingerabdruck)	Nur Personen mit Zugangsberechtigung (Bereich Hausflur, Bereich Büro), Öffnungen werden elektronisch protokolliert, Videoüberwachung Bereich Eingang
Zugang Büro	biometrische Zugangskontrolle (Handvenenscanner)	Nur Personen mit Zugangsberechtigung (Bereich Büro), Öffnungen werden elektronisch protokolliert
Zugang Verwaltung	biometrische Zugangskontrolle (Fingerabdruck)	Nur Personen mit Zugangsberechtigung (Bereich Verwaltung), Öffnungen werden elektronisch protokolliert

Zugang Rechenzentrum Köln	RFID Karte, biometrische Zugangskontrolle	Zugang nur für vorab definierte Personen, Zugang ohne eigene RFID Karte / Fingerabdruck nur nach Voranmeldung und Bestätigung durch Geschäftsführung
Zugang Serverschrank Rechenzentrum	mechanisches Schließsystem	Schlüsselausgabe nur an berechtigte Personen

system-helden GmbH & Co. KG | Wolfstr. 26 53111 Bonn | 0228 - 299 711 70 **Technische und organisatorische**

Maßnahmen Datenschutz

system-helden

Interne Systeme / Rechenzentrum

1.2 Zugangskontrolle

Zugangsbeschränkungen (Zugänge zu EDV Systemen)

System / Systembereich Zugangsschutz

ERP System Passwort / 2-Faktor- Authentifizierung

Dokumentationssystem Passwort (2-Faktor-Authentifizierung bei Zugriff

über externe Netze)

Datenspeicher (Cloud) Passwort / 2-Faktor- Authentifizierung

E-mail Server / Archiv Passwort

Telefonanlage Passwort

Storage und Backupsystem Passwort

MDM Passwort

Seite: 3 von 10

Videüberwachung Passwort

Systemmonitoring Passwort

Kundensysteme Passwort / ggf. Andere Zugangssicherung

Mitarbeitercomputer Passwort / biometrischer Zugangsschutz

1.3 Zugriffskontrolle

System / Systembereich

System / Systembereich Zugangsregelung

ERP System Rechte innerhalb des ERP werden nach Aufgabenbereich und

Berechtigung des Mitarbeiters vergeben, Zugang zu

Konfigurationsdatenbank für alle Mitarbeiter

Dokumentationssystem Benutzerrechte werden nach Aufgabenbereich vergeben,

Zugang auf Kundenakten ist für berechnigte Mitarbeiter

möglich (insbesondere Support, Verwaltung)

Datenspeicher (Cloud) Rechte und Zugriff auf bestimmte Kundendaten werden nach

Aufgabenbereich des Mitarbeiters vergeben, Zugang zu

Konfigurationsdatenbank für alle Mitarbeiter

E-mail Server / Archiv Zugriff nur auf eigene Konten sowie allgemeines Konto,

besondere Kommunikationskonten (billing, info etc.) nur für

berechtigte Mitarbeiter

Telefonanlage Rechte werden auf Grundlage der Aufgaben zugewiesen,

Zugriff auf Faxeingang sowie Anrufhistorie nach

Gruppenrechten möglich

system-helden GmbH & Co. KG | Wolfstr. 26 53111 Bonn | 0228 - 299 711 70 **Technische und organisatorische**

Maßnahmen Datenschutz

Seite: 4 von 10

system-helden

Interne Systeme / Rechenzentrum

System / Systembereich

Zugangsregelung

Storage und Backupsystem Zugang auf allgemeinen Bereich (Downloadordner) für alle

Mitarbeiter, Zugriff auf Datensicherungen und andere Daten

nur für Administratoren

MDM Zugang nur für Administratoren

Videoüberwachung Zugang nur für Geschäftsführung

Systemmonitoring Zugang für ausgewählte berechnigte Mitarbeiter (Support,

Implementierung)

Kundensysteme Zugang für alle Mitarbeiter mit technischen Aufgaben

(Support, Implementierung) nach Absprache mit dem Kunden

Mitarbeitercomputer Mitarbeiter hat vollen Zugriff auf seinen Arbeitscomputer,

Arbeitsvertrag regelt Trennung von privaten und

Firmenzugängen

1.4 Weitergabekontrolle

Der Zugang zu EDV Systemen wird (für interne Systeme) durch technische Maßnahmen wie

Zugriffsprotokolle und durchgängiges Monitoring dauerhaft überwacht. Durch die Installation und Nutzung

eines Geräteverwaltungssystems werden die Vorgaben für die Sicherheit der Geräte dauerhaft überwacht

und können durch den Benutzer nicht verändert werden. Durch Protokollierung der Datenschnittstellen

unserer Systeme sind Datenflüsse nachträglich nachvollziehbar und können, im Falle eines Verstoßes,

genau nachvollzogen werden.

1.5 Trennungsgebot

Seite: 5 von 10

Die für die Verarbeitung innerhalb der Systeme gespeicherten und erhobenen Daten stehen nur innerhalb der genannten Systeme zur Verfügung. Durch die auf Benutzer- und Benutzergruppenebene getroffenen Zugriffsbeschränkungen ist nur befugten Personen Zugriff auf die gespeicherten und verarbeiteten Daten möglich. In den Systeme ERP, Datencloud sowie CMDB sind für jeden Kunden eigenständige Datencontainer (Ordner) eingerichtet, welche ausschließlich die Daten der betroffenen Kunden enthalten.

1.6 Pseudonymisierung

Es liegt keine Pseudonymisierung vor.

1.7 Verschlüsselung

Systemname Systemname

Maßnahme zur Datensicherheit

ERP System Zugriff auf das ERP nur über TLS verschlüsselte

Verbindungen. Datenbank verschlüsselt

Dokumentationssystem Zugriff auf nur innerhalb des internen Netzwerks oder

verschlüsselte Verbindungen (VPN). Datenbank verschlüsselt

system-helden GmbH & Co. KG | Wolfstr. 26 53111 Bonn | 0228 - 299 711 70 **Technische und organisatorische**

Maßnahmen Datenschutz

system-helden

Interne Systeme / Rechenzentrum

Systemname

Maßnahme zur Datensicherheit

Datenspeicher (Cloud) Zugriff auf Cloud nur über TLS verschlüsselte Verbindungen.

E-mail Server / Archiv Zugriff auf den E-Mail Server nur über TLS verschlüsselte

Verbindungen.

Telefonanlage Zugriff nur über internes Netzwerk.

Storage und Backupsystem Zugriff nur über internes Netzwerk.

MDM Zugriff nur über internes Netzwerk oder verschlüsselte
Verbindung (VPN).

Videoüberwachung Zugriff nur über TLS verschlüsselte Verbindungen.

Systemmonitoring Zugriff nur über internes Netzwerk.

Kundensysteme Zugriff nur über internes Netzwerk.

Mitarbeitercomputer Zugriff nur über TLS verschlüsselte Verbindungen von
definierten Anschlüssen (IP Adressen) oder über
verschlüsselte VPN Verbindung.

Datenserver Zugriff nur über separiertes RZ Netzwerk.

RZ Netzwerkmanager Zugriff nur über internes Netzwerk.

MDM (MSP) Zugriff nur über TLS verschlüsselte Verbindungen.

SecureMail Server Zugriff auf den E-Mail Server nur über TLS verschlüsselte
Verbindungen.

Tomedo Cloud Server Zugriff auf den E-Mail Server nur über TLS verschlüsselte
Verbindungen.

3. Verfügbarkeit

3.1 Verfügbarkeitskontrolle

Alle Rechenzentrumsserver sind zusätzlich mit einer redundant ausgeführten Serverinfrastruktur
ausgestattet, welche Ausfälle einzelner Komponenten (z.B. Festplatte, Netzteil, Netzwerkkarte) ausgleicht.

Eine High-Availability Lösung (mehrfach vorhandene Serverhardware für den Fall eines Komplettausfalls) ist
jederzeit installierbar.

3.2 Wiederherstellbarkeit

Systemname Systemname

Maßnahme zur Datensicherheit

ERP System Datensicherungen auf redundante Sicherungssysteme alle 24

Stunden

Dokumentationssysteme Datensicherung auf redundante Sicherungssysteme alle 12

Stunden

system-helden GmbH & Co. KG | Wolfstr. 26 53111 Bonn | 0228 - 299 711 70 **Technische und organisatorische**

Maßnahmen Datenschutz

system-helden Interne Systeme / Rechenzentrum	
Systemname	Maßnahme zur Datensicherheit
Datenspeicher (Cloud)	Datensicherungen auf redundante Sicherungssysteme alle 24 Stunden
E-Mail Server	Datensicherungen auf redundante Sicherungssysteme alle 24 Stunden
E-Mail Archiv	Sicherung auf redundante Sicherungssysteme alle 24 Stunden
Storage- und Backupsystem	Sicherung auf externes Sicherungssystem
MDM	Datensicherung auf redundantes System alle 24 Stunden

Monitoring System	Sicherung auf redundante Sicherungssysteme alle 24 Stunden
Videoüberwachung	Sicherung auf redundante Sicherungssysteme alle 24 Stunden
Datenserver	Datensicherung von bestimmten Daten auf externes Sicherungssystem
Unifi Netzwerkmanager	Sicherung auf externes Sicherungssystem
MDM (MSP)	Datensicherung auf redundantes System alle 24 Stunden
SecureMail Server	Datensicherungen auf redundante Sicherungssysteme alle 24 Stunden
Tomedo Cloud Server	Datensicherungen auf redundante Sicherungssysteme alle 24 Stunden

4. Weiteres

4.1 Auftragskontrolle

Eine Auftragskontrolle erfolgt auf Grundlage einer sorgfältigen Kundenauswahl. Aufträge werden erst nach Bestätigung durch zeichnungsberechtigte Vertreter des Kunden durchgeführt. Für Aufträge, welche einen bestimmten Auftragswert überschreiten wird zusätzlich immer eine gesonderte schriftliche Bestätigung des Kunden eingeholt. Die Durchführung der Aufträge wird durch eine Auftragsverfolgung innerhalb des internen

ERP Systems protokolliert.

4.2 Managementsystems zum Datenschutz

Ein Managementsystem zum Datenschutz ist nicht vorhanden. Datenschutzanfragen sowie

Datenschutzbezogene Vorgänge werden mit dem externen Datenschutzbeauftragten abgesprochen.