TOM 2026.2

gültig vom 01.09.2026 bis 14.10.2026

Änderungshinweise

Ergänzung der Maßnahmen für Verarbeitungen besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) und für Auftraggeber, die einer Berufsgeheimnispflicht nach § 203 StGB unterliegen; Ergänzung Abschnitt 2 (Integrität), Fernwartung, Löschung und Datenträgerentsorgung; Überarbeitung Ziffer 4.2.

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.

Soweit der Auftragnehmer für einen Auftraggeber Verarbeitungen durchführt, die besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO umfassen oder bei denen der Auftraggeber einer Berufsgeheimnispflicht nach § 203 StGB unterliegt, gelten ergänzend die Maßnahmen nach Ziffer 5.

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.

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

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

Zugangsbeschränkungen (Zugänge zu EDV-Systemen)

System / Systembereich	**Zugangsschutz**
ERP System	Passwort / 2-Faktor-Authentifizierung
Dokumentationssystem	Passwort (2-Faktor-Authentifizierung bei Zugriff über externe Netze)

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

Datenspeicher (Cloud)	Passwort / 2-Faktor-Authentifizierung
E-Mail Server / Archiv	Passwort / 2-Faktor-Authentifizierung
Telefonanlage	Passwort
Storage und Backupsystem	Passwort / 2-Faktor-Authentifizierung
MDM	Passwort / 2-Faktor-Authentifizierung
Videoüberwachung	Passwort
Systemmonitoring	Passwort / 2-Faktor-Authentifizierung
Kundensysteme	Passwort und 2-Faktor-Authentifizierung, personalisierte Administrationskonten; Sammelkonten werden nicht verwendet
Mitarbeitercomputer	Passwort / biometrischer Zugangsschutz
Datenserver	Passwort / 2-Faktor-Authentifizierung, Zugriff nur aus dem separierten RZ-Netzwerk
RZ Netzwerkmanager	Passwort / 2-Faktor-Authentifizierung
MDM (MSP)	Passwort / 2-Faktor-Authentifizierung
SecureMail Server	Passwort / 2-Faktor-Authentifizierung
Tomedo Cloud Server	Passwort und 2-Faktor-Authentifizierung, personalisierte Administrationskonten, Zugriff nur aus dem separierten RZ-Netzwerk oder über VPN

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

System / Systembereich	Zugangsregelung
ERP System	Rechte innerhalb des ERP werden nach Aufgabenbereich und Berechtigung des Mitarbeiters vergeben, Zugang zur Konfigurationsdatenbank nur für Administratoren
Dokumentationssystem	Benutzerrechte werden nach Aufgabenbereich vergeben, Zugang auf Kundenakten ist für berechtigte Mitarbeiter möglich (insbesondere Support, Verwaltung)
Datenspeicher (Cloud)	Rechte und Zugriff auf bestimmte Kundendaten werden nach Aufgabenbereich des Mitarbeiters vergeben, Zugang zur Konfigurationsdatenbank nur für Administratoren
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
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 berechtigte Mitarbeiter (Support, Implementierung)
Kundensysteme	Der Zugriff ist auf einen namentlich benannten Kreis von Mitarbeitern beschränkt, der dem jeweiligen Auftraggeber auf Anforderung mitgeteilt wird. Die Zuweisung erfolgt mandantenbezogen nach dem Grundsatz der geringsten Rechte; Berechtigungen werden mindestens jährlich sowie bei jedem Austritt oder Aufgabenwechsel überprüft und bei Wegfall des Bedarfs unverzüglich entzogen. Zugriffe werden protokolliert.

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

Mitarbeitercomputer	Mitarbeiter hat vollen Zugriff auf seinen Arbeitscomputer, Arbeitsvertrag regelt Trennung von privaten und Firmenzugängen
Datenserver	Zugriff ausschließlich für Administratoren, mandantenbezogene Trennung, Protokollierung der Zugriffe
RZ Netzwerkmanager	Zugang nur für Administratoren
MDM (MSP)	Zugang nur für Administratoren
SecureMail Server	Zugang nur für Administratoren
Tomedo Cloud Server	Zugriff ausschließlich für den nach Ziffer 5.1 benannten Kreis technischer Mitarbeiter, mandantenbezogene Trennung, Protokollierung sämtlicher Zugriffe, Auswertung der Protokolle bei Anlass

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.

Die Weitergabe personenbezogener Daten an Dritte erfolgt ausschließlich auf dokumentierte Weisung des jeweiligen Auftraggebers. Der Versand von Datenträgern an Dritte, insbesondere im Rahmen von Garantie- oder Austauschvorgängen (RMA), ist nach Maßgabe der Ziffer 5.3 unzulässig, solange die Datenträger personenbezogene Daten enthalten.

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 Systemen ERP, Datencloud sowie CMDB sind für jeden Kunden eigenständige Datencontainer (Ordner) eingerichtet, welche ausschließlich die Daten der betroffenen Kunden enthalten.

Kundensysteme werden logisch voneinander getrennt betrieben. Eine mandantenübergreifende Zusammenführung von Daten findet nicht statt.

Eine Pseudonymisierung der im Auftrag verarbeiteten Daten findet nicht statt. Der Auftragnehmer verarbeitet die

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

Daten seiner Auftraggeber nicht inhaltlich, sondern erhält im Rahmen der Administration und Fehlerbehebung anlassbezogen Zugriff auf Bestandsdaten in den Systemen der Auftraggeber. Eine Pseudonymisierung würde den Zweck der beauftragten Leistung (Identifikation und Behebung konkreter Fehler an konkreten Datensätzen) vereiteln und ist daher nicht geeignet. Als kompensierende Maßnahmen wirken die Zugriffsbeschränkungen nach Ziffer 1.3, die Protokollierung nach Ziffer 2.1 sowie die Beschränkung der Fernwartung nach Ziffer 5.2.

Systemname	**Maßnahme zur Datensicherheit**
ERP System	Zugriff auf das ERP nur über TLS-verschlüsselte Verbindungen. Datenbank verschlüsselt
Dokumentationssystem	Zugriff nur innerhalb des internen Netzwerks oder über verschlüsselte Verbindungen (VPN). Datenbank verschlüsselt
Datenspeicher (Cloud)	Zugriff auf Cloud nur über TLS-verschlüsselte Verbindungen. Speicherung verschlüsselt (Verschlüsselung ruhender Daten).
E-Mail Server / Archiv	Zugriff auf den E-Mail Server nur über TLS-verschlüsselte Verbindungen. Datenbank und Archivspeicher verschlüsselt.
Telefonanlage	Zugriff nur über internes Netzwerk.
Storage und Backupsystem	Zugriff nur über internes Netzwerk. Sämtliche Datensicherungen werden verschlüsselt gespeichert; die Schlüsselverwaltung erfolgt getrennt vom Sicherungsmedium.
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. Fernzugriffe ausschließlich über verschlüsselte Verbindungen.

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

Mitarbeitercomputer	Zugriff nur über TLS-verschlüsselte Verbindungen von definierten Anschlüssen (IP-Adressen) oder über verschlüsselte VPN-Verbindung. Die lokalen Datenträger sämtlicher Arbeitsgeräte sind vollständig verschlüsselt (Festplattenverschlüsselung); die Verschlüsselung wird über das Geräteverwaltungssystem erzwungen und überwacht.
Datenserver	Zugriff nur über separiertes RZ-Netzwerk. Datenträger verschlüsselt.
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 ausschließlich über verschlüsselte Verbindungen (TLS bzw. VPN). Datenträger und Datenbank verschlüsselt; Datensicherungen verschlüsselt.

Eingaben, Änderungen und Löschungen in den Systemen des Auftragnehmers werden mit Benutzerkennung und Zeitstempel protokolliert. Administrative Zugriffe auf Kundensysteme, insbesondere auf den Datenserver und den Tomedo Cloud Server, werden gesondert protokolliert. Die Protokolle sind gegen nachträgliche Veränderung geschützt und werden für einen Zeitraum von mindestens 90 Tagen aufbewahrt. Eine Auswertung erfolgt anlassbezogen, insbesondere bei Verdacht auf eine Verletzung des Schutzes personenbezogener Daten.

Die Übertragung personenbezogener Daten erfolgt ausschließlich über verschlüsselte Verbindungen nach dem Stand der Technik. Der Transport von Datenträgern erfolgt nur in verschlüsselter Form. Schnittstellen zu externen Systemen sind dokumentiert; Datenflüsse sind über die Protokollierung nach Ziffer 1.4 nachvollziehbar.

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.

Das Rechenzentrum verfügt über eine unterbrechungsfreie Stromversorgung, Netzersatzanlage, Klimatisierung sowie Brandfrüherkennung und Löschanlage.

Systemname	**Maßnahme zur Datensicherheit**

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

ERP System	Datensicherungen auf redundante Sicherungssysteme alle 24 Stunden
Dokumentationssysteme	Datensicherung auf redundante Sicherungssysteme alle 12 Stunden
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

Die Wiederherstellbarkeit der Datensicherungen wird mindestens jährlich durch dokumentierte Rücksicherungstests überprüft. Das Ergebnis wird schriftlich festgehalten und im Rahmen der Überprüfung nach Ziffer 4.2 ausgewertet.

Eine Auftragskontrolle erfolgt auf Grundlage einer sorgfältigen Kundenauswahl. Aufträge werden erst nach Bestätigung

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

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.

Sämtliche Mitarbeiter werden vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b, Art. 32 Abs. 4 DSGVO) und mindestens jährlich zum Datenschutz und zur Informationssicherheit geschult. Die Verpflichtungen und Schulungsteilnahmen werden dokumentiert.

Unterauftragnehmer werden vor ihrem Einsatz auf die Einhaltung eines angemessenen Schutzniveaus geprüft; die Prüfung wird dokumentiert. Ihnen werden dieselben Datenschutzpflichten vertraglich auferlegt, die den Auftragnehmer gegenüber seinen Auftraggebern treffen.

Der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt. Datenschutzanfragen sowie datenschutzbezogene Vorgänge werden mit dem externen Datenschutzbeauftragten abgestimmt und dokumentiert.

Zur Erfüllung von Art. 32 Abs. 1 lit. d DSGVO überprüft, bewertet und evaluiert der Auftragnehmer die Wirksamkeit der technischen und organisatorischen Maßnahmen nach folgendem Verfahren:

- Überprüfung dieses Dokuments mindestens einmal jährlich sowie anlassbezogen bei wesentlichen Änderungen der Systeme, Prozesse oder Unterauftragnehmer; das Ergebnis wird mit Datum und Fassungsnummer dokumentiert.
- Jährliche Überprüfung der Berechtigungen nach Ziffer 1.3 sowie der Protokolle nach Ziffer 2.1 auf Stichprobenbasis.
- Jährliche dokumentierte Rücksicherungstests nach Ziffer 3.2.
- Dokumentation und Auswertung sämtlicher Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten sowie Ableitung von Maßnahmen.
- Jährliche Prüfung der eingesetzten Unterauftragnehmer nach Ziffer 4.1.

Die Ergebnisse werden schriftlich festgehalten und den Auftraggebern auf Anforderung in geeigneter Weise nachgewiesen.

Die Maßnahmen dieser Ziffer gelten ergänzend für Verarbeitungen, die besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO umfassen, insbesondere Gesundheitsdaten, sowie für Auftraggeber, die einer Berufsgeheimnispflicht nach § 203 StGB unterliegen.

Mitarbeiter, die im Rahmen ihrer Tätigkeit Zugriff auf Daten erhalten können, die einer Berufsgeheimnispflicht unterliegen, werden vor der ersten Tätigkeit gesondert zur Geheimhaltung verpflichtet und über die Strafbarkeit einer unbefugten Offenbarung nach § 203 StGB belehrt. Die Verpflichtung wird schriftlich dokumentiert und dem Auftraggeber auf Anforderung nachgewiesen. Sie gilt über die Beendigung des Beschäftigungsverhältnisses hinaus fort.

Der Kreis der so verpflichteten Mitarbeiter wird gesondert geführt. Nur diese Mitarbeiter erhalten Zugriff auf die betreffenden Kundensysteme. Der jeweilige Auftraggeber erhält auf Anforderung eine namentliche Aufstellung der zugriffsberechtigten Personen.

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD

Unterauftragnehmer, die Zugriff auf solche Daten erhalten können, werden entsprechend § 203 Abs. 4 Satz 3 StGB vertraglich zur Geheimhaltung verpflichtet und zur Weitergabe dieser Verpflichtung an ihre eigenen Beschäftigten und Unterauftragnehmer angehalten.

Mitarbeiter mit Zugriff auf besondere Kategorien personenbezogener Daten werden zusätzlich zur allgemeinen Schulung nach Ziffer 4.1 gesondert zum Umgang mit diesen Daten geschult (§ 22 Abs. 2 Satz 2 Nr. 3 BDSG).

Fernwartungszugriffe auf Systeme des Auftraggebers erfolgen ausschließlich über verschlüsselte Verbindungen und über personalisierte Zugänge. Ein dauerhafter, unbeaufsichtigter Zugriff besteht nicht.

Die Fernwartungssitzung wird durch den Auftraggeber freigegeben. Die eingesetzte Software ermöglicht dem Auftraggeber, die durchgeführten Arbeiten am Bildschirm zu verfolgen und die Sitzung jederzeit zu beenden.

Jede Fernwartungssitzung wird mit Zeitpunkt, Dauer, ausführendem Mitarbeiter und Gegenstand der Tätigkeit protokolliert. Die Protokolle werden mindestens 90 Tage aufbewahrt und dem Auftraggeber auf Anforderung zur Verfügung gestellt.

Eine Kenntnisnahme von Inhaltsdaten erfolgt nur, soweit dies zur Erbringung der beauftragten Leistung erforderlich ist. Eine Speicherung oder lokale Zwischenspeicherung von Inhaltsdaten auf Geräten des Auftragnehmers findet nicht statt; die Übertragung von Dateien aus der Fernwartungssitzung ist auf das erforderliche Maß beschränkt und wird protokolliert.

Daten, die dem Auftragnehmer im Rahmen der Auftragsverarbeitung überlassen wurden, werden nach Beendigung des Auftrags nach Wahl des Auftraggebers herausgegeben oder gelöscht. Die Löschung erfolgt einschließlich vorhandener Datensicherungen und Protokolle, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht, und wird dem Auftraggeber auf Anforderung bestätigt.

Datenträger, die personenbezogene Daten eines Auftraggebers enthalten oder enthalten haben, werden nicht an Hersteller oder Dritte herausgegeben. Im Rahmen von Garantie- oder Austauschvorgängen verbleiben betroffene Datenträger beim Auftraggeber oder werden nachweislich vernichtet.

Die Vernichtung von Datenträgern erfolgt nach DIN 66399 in der für die jeweilige Schutzklasse erforderlichen Sicherheitsstufe; für Datenträger mit besonderen Kategorien personenbezogener Daten mindestens Schutzklasse 3. Über die Vernichtung wird ein Nachweis erstellt.

Papierunterlagen werden in verschlossenen Sammelbehältern erfasst und datenschutzgerecht vernichtet.

system-helden Systemhaus GmbH
Wolfstr. 26
53111 Bonn
Deutschland

Telefon: +49 228 299 711 70
Mail: hello@system-helden.de
Web: www.system-helden.de

Ust-ID: DE364021447
HR Nr: HRB 31011
Registergericht: Bonn

Apobank
IBAN: DE55 3006 0601 0105 3563 00
BIC: DAAEDEDD