Technische Schutzfunktionen von Hanware

Beschreibung der Sicherheitsfunktionen der Software als Hilfe für das Verzeichnis der technischen und organisatorischen Maßnahmen

Information des Herstellers – kein Vertrags- und kein Rechtstext

Programmversion	ab 42.01
Stand	10.10.2026
Hersteller	Hanware GmbH
Bezug	Art. 30 und 32 DSGVO (Verzeichnis, Sicherheit der Verarbeitung)

Diese Information ersetzt keine rechtliche Beratung und keine Prüfung durch den Datenschutzbeauftragten.

1 Zweck dieser Information

Wer personenbezogene Daten verarbeitet, muss geeignete technische und organisatorische Maßnahmen treffen und sie im Verzeichnis der Verarbeitungstätigkeiten beschreiben. Diese Information zeigt, welche **Schutzfunktionen die Software Hanware** dafür mitbringt und wo **organisatorische Maßnahmen des Unternehmens** nötig bleiben. Sie können die Beschreibungen sinngemäß in Ihr Verzeichnis übernehmen.

Abgrenzung

Diese Information ist **kein Vertragsbestandteil** und **kein Rechtstext**. Sie ersetzt weder den Vertrag zur Auftragsverarbeitung noch die Datenschutzerklärung der Hanware GmbH; diese finden Sie in der Dokumentenzentrale unter „Rechtliches“. Verantwortlich für die Verarbeitung und für die Auswahl und Umsetzung der Maßnahmen bleibt das Unternehmen, das Hanware einsetzt.

Hanware wird in der Regel im Netz des Unternehmens oder bei dessen Dienstleister betrieben: Die Daten liegen auf einem Datenbankserver, die Dateien des Dokumentenarchivs in einem Dateiordner. Physische Sicherheit, Netzwerk, Server und Betriebssysteme liegen damit in der Verantwortung des Unternehmens.

2 Zugang und Zugriff

Funktion	Beschreibung
Persönliche Anmeldung	Jeder Benutzer meldet sich mit eigener Benutzernummer und eigenem Kennwort an. Alle Vorgänge werden dem angemeldeten Benutzer zugeordnet.
Berechtigungen	Funktionen und Menüs lassen sich je Benutzer freigeben oder sperren. Kritische Funktionen – Abschlüsse aufheben, gesperrte Belege entsperren, Nummernkreise setzen, TSE-Einstellungen – sind eigene Berechtigungen. Jede Änderung von Benutzerrechten wird mit altem und neuem Wert protokolliert.
Kennwörter	Kennwörter werden nicht im Klartext gespeichert und nie in Protokolle geschrieben; das Setzen, Ändern und Löschen eines Kennworts wird protokolliert.
Schutz der Anmeldung	Die Anmeldeabfrage ist gegen das Einschleusen von Datenbankbefehlen gesichert.
Hersteller-Support	Für den Support gibt es einen gesonderten Zugang; jede Anmeldung damit wird mit Arbeitsplatz und Zeitpunkt protokolliert. Wartungs- und Datenbankwerkzeuge sind nur mit Support-Kennwort aufrufbar; Ausführung und abgelehnte Versuche werden protokolliert.
Automatische Anmeldungen	Betrieb ohne Anmeldemaske, mobile Ausgabe und Druckdienst werden mit Weg, Arbeitsplatz und Zeitpunkt protokolliert; der Druckdienst erhält keinen Zugriff auf Menüs.
Trennung der Mandanten	Jeder Mandant hat eine eigene Datenbank und eine eigene Protokolldatenbank.

3 Eingabe- und Änderungskontrolle

Die Protokollierung ist **fest eingeschaltet** und kann vom Anwender nicht abgeschaltet werden. Protokolleinträge enthalten Benutzer, Arbeitsplatz bzw. Quelle, Zeitpunkt und bei Änderungen den alten und neuen Wert.

Protokoll	Inhalt
Belegprotokoll	Speicherung, Änderung, Druck und Versand von Belegen und Positionen
Änderungsprotokoll	Feldänderungen an Belegen, Rechten, Kennwörtern (ohne Kennwortwert), Einstellungen, Kassen- und Abschlussvorgängen sowie Anmeldungen mit Sonderzugang
Zahlungsprotokoll	Löschung, Storno und Umbuchung von Zahlungen mit vollständigem Vorzustand
Löschsicherung	vollständige Kopie jedes gelöschten Datensatzes (Belege, Positionen, Zahlungen, Adressen, Artikel)

Protokolle und Löschsicherungen lassen sich weder über die Oberfläche noch über die Löschfunktionen des Programms entfernen.

4 Integrität und Schutz vor Verlust

- Buchungsrelevante Belege mit Nummer werden nicht gelöscht, sondern storniert; abgeschlossene Zeiträume sind gegen Änderung gesperrt.
- Gelöschte Datensätze werden gekennzeichnet und vollständig gesichert; auf Datenbankebene sichern Trigger jede gelöschte Zeile der Kerntabellen.
- Abgelegte Dokumente werden beim Löschen archiviert statt entfernt.
- Die Uhrzeit der Arbeitsplätze wird bei der Anmeldung mit der Serverzeit verglichen; bei Abweichung erscheint ein Hinweis.

Datensicherung

Hanware bietet eine Datensicherung der Mandantendatenbank und der Protokolldatenbank an. Zugangsdaten werden dafür nicht dauerhaft im Klartext abgelegt; temporäre Steuerdateien werden nach dem Lauf entfernt. Zeitplan, Aufbewahrung der Sicherungen außer Haus, Verschlüsselung der Sicherungsmedien und Wiederherstellungstests organisiert das Unternehmen. Der Dokumentenordner gehört in die Sicherung des Unternehmens.

5 Aufbewahrung und Löschung personenbezogener Daten

Steuerliche und handelsrechtliche Aufbewahrungspflichten gehen der Löschung vor, solange die Fristen laufen. Hanware löscht deshalb buchungsrelevante Daten nicht und bietet **keine automatische Löschung** nach Ablauf der Aufbewahrungsfristen. Für Löschanfragen Betroffener und die Bereinigung nach Fristablauf legt das Unternehmen ein Verfahren fest; bei Bedarf unterstützt der Hanware-Support.

6 Maßnahmen des Unternehmens

Die Schutzfunktionen der Software wirken nur zusammen mit organisatorischen und technischen Maßnahmen des Unternehmens:

Zugang und Rechte

- ☐ Für jeden Benutzer ein eigenes, sicheres Kennwort vergeben; keine Sammelkonten
- ☐ Berechtigungen nach dem Prinzip der minimalen Rechte vergeben und jährlich prüfen
- ☐ Benutzer ausgeschiedener Mitarbeiter sofort sperren
- ☐ Bildschirmsperre an den Arbeitsplätzen
- ☐ Support-Zugänge und Fernwartung nur im Bedarfsfall freigeben

Server, Netz und Sicherung

- ☐ Datenbankserver und Dokumentenordner nur für berechtigte Konten zugänglich
- ☐ Verbindung von außen nur über gesicherte Wege, z. B. VPN
- ☐ Betriebssysteme, Datenbankserver und Hanware aktuell halten
- ☐ Sicherungen verschlüsselt und außer Haus aufbewahren, Wiederherstellung testen
- ☐ Exportdateien und Ausdrucke mit personenbezogenen Daten geschützt ablegen

7 Grenzen

Die folgenden Punkte sollten Sie bei der Bewertung Ihrer Maßnahmen berücksichtigen:

Thema	Stand	Empfehlung
Standard bei Berechtigungen	Funktionen, für die bei einem Benutzer kein Recht ausdrücklich gesetzt ist, stehen ihm zur Verfügung.	Rechte neuer Benutzer bewusst einrichten und prüfen.
Benutzer ohne Kennwort	Die Anmeldung ohne Kennwort ist möglich, wenn für einen Benutzer keines vergeben ist; sie wird protokolliert.	Für alle Benutzer Kennwörter vergeben.
Ablage der Kennwörter	Kennwörter werden kodiert gespeichert; die Kodierung ist kein kryptografisches Hashverfahren.	Zugriff auf den Datenbankserver streng beschränken.
Betrieb ohne Anmeldemaske	Der Bearbeiter ist dann nur über den Arbeitsplatz zuzuordnen.	Nur dort einsetzen, wo ein Arbeitsplatz genau einer Person zugeordnet ist.
Zusatzprogramme	Einzelne Zusatzprogramme (z. B. Datensicherung, E-Rechnung, Bankabruf) erhalten die Verbindungsdaten zur Datenbank beim Aufruf.	Arbeitsplätze vor fremdem Zugriff schützen; eine gesicherte Übergabe ist vorgesehen.
Sicherungsdateien	Die von Hanware erstellten Sicherungsdateien sind nicht verschlüsselt.	Sicherungsziel schützen bzw. Medien verschlüsseln.

Thema	Stand	Empfehlung
Dokumentenordner	Dateien sind im Dateisystem gespeichert und außerhalb des Programms nur durch die Rechte des Betriebssystems geschützt.	Ordnerrechte einschränken.
Löschung nach Fristablauf	Keine automatische Löschung.	Verfahren organisatorisch festlegen.

Hinweis: Diese Information beschreibt Funktionen der Software Hanware ab Version 42.01 als Hilfe für das Verzeichnis der technischen und organisatorischen Maßnahmen des Anwenders. Sie ist kein Vertrags- oder Rechtstext, begründet keine Zusicherung von Eigenschaften und ersetzt keine rechtliche Beratung. Maßgeblich für die Auftragsverarbeitung ist allein der Vertrag zur Auftragsverarbeitung der Hanware GmbH. Hanware GmbH · Stand 10.10.2026