HOFFROGGE

Technische und organisatorische Maßnahmen von Hoffrogge nach Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 (1) b DSGVO)

1.1. Zutrittskontrolle

1.1.1. Server

- Die Serverräume sind fensterlos und durch eine Einbruchmeldeanlage geschützt.
- Die Serverräume werden durch ein elektronisches Schließsystem (personalisiertes RFID-System) geschützt.
- Sowohl der Zutritt als auch die Verweigerung des Zutritts zu den Serverräumen werden protokolliert.
- Die Serverräume sind durch zusätzliche mechanische Schlösser geschützt. Zu jedem Schloss gibt es zwei Schlüssel, die in einem Safe aufbewahrt werden.
- Nur eine begrenzte Anzahl von Personen hat Zutritt zu den Serverräumen (Geschäftsführung, IT-Management und IT-Administratoren).
- Bei Wartungs- oder Reinigungsarbeiten wird das externe Personal von Hoffrogge Mitarbeitenden beim Zutritt und während der gesamten Präsenz in den Serverräumen begleitet.
- Der Zutritt von externem Personal wird protokolliert.

1.1.2. Personal Computer

- Das Bürogebäude ist durch eine Einbruchmeldeanlage geschützt; im Alarmfall wird eine Alarmmeldekette von Hoffrogge durch eine dauerhaft besetzte Einsatzleitstelle informiert.
- Das Bürogebäude ist durch ein elektronisches Schließsystem (personalisiertes RFID-System) geschützt.
- Sowohl der Zutritt als auch die Verweigerung des Zutritts zum Bürogebäude werden protokolliert.
- Das Bürogebäude ist durch zusätzliche mechanische Schlösser geschützt und die Schlüsselübergabe wird protokolliert.
- Das Betriebsgelände ist durch ein Videoüberwachungssystem geschützt.
- Externe Besucher werden am Eingang des Bürogebäudes von Hoffrogge Mitarbeitenden empfangen und von ihrem Ansprechpartner beim Zutritt begleitet.
- Externe Besucher werden im Gästebuch protokolliert.

1.2. Zugangskontrolle

- Die IT-Systeme, die zur Verarbeitung der Unternehmensdaten verwendet werden, sind durch Benutzernamen und Passwörter geschützt.
- Die IT-Systeme sind durch separate Admin-Accounts geschützt, die sich vom regulären Benutzerkonto des Administrators unterscheiden.
- Hoffrogge sorgt für die Einhaltung von verbindlichen und sicheren Passwort-Regeln.
- Die Computerbildschirme werden automatisch nach 15 Minuten Inaktivität gesperrt und können nur mit einem Passwort entsperrt werden.
- Die Mitarbeitenden müssen ihre Computer bei jedem Verlassen ihres Arbeitsplatzes sperren.
- Die Aktualität der Zugangsberechtigungen wird regelmäßig überprüft.
- Die für die Datenverarbeitung eingesetzten IT-Systeme sind durch eine Firewall geschützt.

1.3. Zugriffskontrolle

- Hoffrogge sieht ein differenziertes Berechtigungskonzept vor, das den Zugriff der Mitarbeitenden auf die Daten des Unternehmens regelt.
- Hoffrogge stellt sicher, dass die Zugangsberechtigung von Mitarbeitenden bei internen Stellenwechseln und/oder Kündigungen aktualisiert bzw. widerrufen wird.
- Hoffrogge unterhält getrennte Produktions- und Prüfsysteme.

2. Integrität (Art. 32 (1) b DSGVO)

2.1. Weitergabekontrolle

- Alle Datentransfers werden über eine verschlüsselte Verbindung übertragen.
- Der Datentransfer wird protokolliert.
- Den Mitarbeitern von Hoffrogge ist es untersagt, die Daten des Unternehmens auf ihren eigenen privaten Geräten zu verwenden (kein "bring your own device").

2.2 Eingabekontrolle

- Hoffrogge regelt und dokumentiert die Eingabeberechtigungen über die Benutzeridentifikation und Berechtigungskonzepte.
- Die Eingaben von personenbezogenen Daten werden protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 (1) b, c DSGVO)

3.1. Verfügbarkeitskontrolle

- Die Serverräume sind durch Brandschutztüren geschützt.
- Die Serverräume mit Sensoren (Hitze, Wasser) ausgestattet.
- Die Serverräume sind an eine zentrale Einsatzleitstelle angeschlossen.
- Die Außenwände der Serverräume sind massive Wände (Beton, Ziegel).
- Die Serverräume sind redundant klimatisiert.
- Die Serverräume sind mit unterbrechungsfreier Stromversorgung (USV) ausgestattet.
- Die Funktionalität der USV wird regelmäßig getestet.
- Alle kritischen Systeme werden jeweils redundant in unterschiedlichen Brandabschnitten / Gebäudeteilen betrieben.
- Hoffrogge setzt eine etablierte Backup-Strategie um.
- Alle IT-Systeme sind vor Datenverlust bzw. unberechtigtem Zugriff geschützt.
- Hoffrogge sorgt für ein dokumentiertes Notfallkonzept.

3.2. Datenwiederherstellung

- Hoffrogge hat Redundanz auf allen kritischen Systemen, um die Nichtverfügbarkeit von Daten oder Diensten zu vermeiden.
- Hoffrogge führt regelmäßige Wiederherstellungstests durch.
- Ein nach ISO 27001 genehmigter Disaster Recovery Plan beschreibt, wie mit unerwarteten Situationen wie Störungen, Notfällen, Krisen oder Katastrophen umgegangen wird.

4. Verfahren für die regelmäßige Prüfung, Bewertung und Evaluierung (Art. 32 (1) d DSGVO; Art. 25 (1) DSGVO; Art. 28 DSGVO)

4.1. Datenschutz-Management

- Hoffrogge hat einen internen, zertifizierten Datenschutzbeauftragten (DSB) benannt:
  Name: Nina Weißflog
  Tel.: +49 44 31 70 77 179
  E-Mail: dataprotection@hoffrogge.com
- Die Mitarbeitenden von Hoffrogge werden regelmäßig im Bereich Datenschutz geschult (E-Learning, Schulung durch DSB).
- Die Mitarbeitenden von Hoffrogge haben sich zur Vertraulichkeit und auf das Datengeheimnis verpflichtet (schriftlich).

4.2. Sicherheitsvorfall-Management

- Hoffrogge implementierte ein Information Security Management System (ISMS) nach ISO 27001.
- Das ISMS beinhaltet ein definiertes Verfahren für die Behandlung von Vorfällen, das Lernen aus Vorfällen und die Sammlung von Beweisen.

4.3. Datenschutzfreundliche Voreinstellungen

- Hoffrogge setzt datenschutzfreundliche Voreinstellungen, z.B. zur Datenminimierung und Verarbeitung personenbezogener Daten nur für einen bestimmten Zweck, um.
- Der Zugriff auf diese Daten ist durch Berechtigungskonzepte streng limitiert.

4.4. Auftrags- oder Vertragssteuerung

- Es erfolgt keine Datenverarbeitung durch Dritte gemäß Art. 28 DSGVO ohne entsprechende Zustimmung oder Weisung des Auftraggebers.
- Hoffrogge sieht klare und eindeutige vertragliche Regelungen, ein formalisiertes Auftragsmanagement sowie strenge Vorgaben bei der Auswahl von Dienstleistern vor.

Zertifikat ISO/IEC 27001:2022 Hoffrogge GmbH (nur zu Informationszwecken)

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2022**

Zertifikat-Registrier-Nr. **01 153 1700382**

Unternehmen: **Hoffrogge GmbH**
Am Spascher See 2
27793 Wildeshausen
Deutschland

Geltungsbereich: Entwicklung von Software-Lösungen und IT-Prozessen für das Category und Sales Management sowie Bereitstellung von Rechenzentrumsdiensten.

Erklärung zur Anwendbarkeit (SoA) vom 27.08.2025 – Vers. 5

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2022 erfüllt sind.

Gültigkeit: Dieses Zertifikat ist gültig vom 11.12.2023 bis 10.12.2026.
Erstzertifizierung 2017

17.10.2025

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Genau. Richtig.