HOFFROGGE

Technical and organisational measures of Hoffrogge pursuant to Art. 32 GDPR

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

1.1. Physical access control

1.1.1. Server

- The server rooms have no windows and are protected by an intruder alarm system.
- The server rooms are protected by an electronic locking system (personalised RFID system).
- Both access and denial of access to the server rooms are logged.
- The server rooms are protected by additional mechanical locks. Each lock has two keys, which are kept in a safe.
- Only a limited number of people have access to the server rooms (CEO, IT management and IT administrators).
- During maintenance or cleaning work, external personnel are accompanied by Hoffrogge employees when entering and throughout their entire presence in the server rooms.
- The access of external personnel is logged.

1.1.2. Personal computers

- The office building is protected by an intruder alarm system; in the event of an alarm, an alarm notification chain from Hoffrogge is informed by a permanently manned operations control centre.
- The office building is protected by an electronic locking system (personalised RFID system).
- Both access and refusal of access to the office building are logged.
- The office building is protected by additional mechanical locks and key handover is logged.
- The company premises are protected by a video surveillance system.
- External visitors are welcomed at the entrance to the office building by Hoffrogge employees and accompanied by their contact person upon entry.
- External visitors are recorded in the guest book.

1.2. System access control

- The IT systems used to process company data are protected by username and password.
- The IT systems are protected by separate admin accounts that are different from the administrator's regular user account.
- Hoffrogge ensures compliance with binding and secure password rules.
- Computer screens are automatically locked after 15 minutes of inactivity and can only be unlocked with a password.
- Employees must lock their computers whenever they leave their workstation.
- The validity of access authorisations is checked regularly.
- The IT systems used for data processing are protected by a firewall.

1.3. Data access control

- Hoffrogge provides a differentiated authorisation concept that regulates employees' access to company data.
- Hoffrogge ensures that employees' access authorisations are updated or revoked in the event of internal job changes and/or resignations.
- Hoffrogge maintains separate production and testing systems.

2. Integrity (Art. 32 (1) b DSGVO)

2.1. Disclosure control

- All data transfers are transmitted via an encrypted connection.
- The data transfer is logged.
- Hoffrogge employees are prohibited from using company data on their own private devices (no ‘bring your own device’).

2.2 Input control

- Hoffrogge regulates and documents input authorisations via user identification and authorisation concepts.
- The entry of personal data is logged.

3. Availability and resilience (Art. 32 (1) b, c DSGVO)

3.1. Availability control

- The server rooms are protected by fire doors.
- The server rooms are equipped with sensors (heat, water).
- The server rooms are connected to a central control centre.
- The outer walls of the server rooms are solid walls (concrete, brick).
- The server rooms have redundant air conditioning.
- The server rooms are equipped with uninterruptible power supply (UPS).
- The functionality of the UPS is tested regularly.
- All critical systems are operated redundantly in different fire compartments / parts of the building.
- Hoffrogge implements an established backup strategy.
- All IT systems are protected against data loss and unauthorised access.
- Hoffrogge ensures a documented emergency plan.

3.2. Data recovery

- Hoffrogge has redundancy on all critical systems to prevent the unavailability of data or services.
- Hoffrogge performs regular recovery tests.
- An ISO 27001-approved disaster recovery plan describes how to deal with unexpected situations such as disruptions, emergencies, crises or disasters.

4. Procedures for regular review, assessment and evaluation (Art. 32 (1) d DSGVO; Art. 25 (1) DSGVO; Art. 28 DSGVO)

4.1. Data protection management

- Hoffrogge has appointed an internal, certified data protection officer (DPO):
  Name: Nina Weißflog
  Phone: +49 44 31 70 77 179
  E-mail: dataprotection@hoffrogge.com
- Hoffrogge employees receive regular training in data protection (e-learning, training by DSB).
- Hoffrogge employees have committed themselves to confidentiality and data secrecy (in writing).

4.2. Incident response management

- Hoffrogge implemented an Information Security Management System (ISMS) in accordance with ISO 27001.
- The ISMS includes a defined procedure for handling incidents, learning from incidents and collecting evidence.

4.3. Privacy-friendly default settings

- Hoffrogge implements privacy-friendly default settings, e.g. for data minimisation and processing of personal data only for a specific purpose.
- Access to this data is strictly limited by authorisation concepts.

4.4. Order or contract management

- No data processing by third parties shall take place in accordance with Art. 28 GDPR without the corresponding consent or instruction of the client.
- Hoffrogge envisages clear and unambiguous contractual provisions, formalised contract management and strict guidelines for the selection of service providers.

Certificate ISO/IEC 27001:2022 Hoffrogge GmbH (only for information purposes)

Certificate

Standard **ISO/IEC 27001:2022**

Certificate Registr. No. **01 153 1700382**

Certificate Holder: **Hoffrogge GmbH**
Am Spascher See 2
27793 Wildeshausen
Germany

Scope: Development of software solutions and IT-processes for category and sales management as well as provision of data center services.

Statement of Applicability (SoA) of 27th of August.2025 – Vers. 5

Proof has been furnished by means of an audit that the requirements of ISO/IEC 27001:2022 are met.

Validity: The certificate is valid from 2023-12-11 until 2026-12-10.
First certification 2017

2025-10-17

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

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

TÜVRheinland®
Precisely Right.