Kilchenmann AG – Measures for Information Security

Table of Contents

1. Legal Provisions

Data handling at Kilchenmann AG follows the legal requirements, since 01.09.2023 according to the revised FADP (Federal Act on Data Protection). In addition to the existing measures, a processing register was introduced, processes were revised, and employees were trained.

2. Employee Obligation to Data Confidentiality

Employees of Kilchenmann AG are bound by contractually regulated confidentiality agreements and receive regular training on security, emergency, and confidentiality topics.

3. Technical and Organisational Measures

3.1. Technical Measures

3.1.1. Data Centre Security

Kilchenmann AG operates two data centre rooms at its headquarters in Kehrsatz-Bern.
Access to the data centre is restricted to authorised personnel and protected by a monitoring system. Building access is monitored 24/7 by an alarm system and a security service.
Uninterrupted power supply is ensured through a UPS system (short-term) and an emergency power generator (medium-term), both tested monthly.

3.1.2. Patch Management

All components of the IT infrastructure receive security-relevant updates during the monthly maintenance window. Critical vulnerabilities are closed immediately once identified.

3.1.3. Network Security

Kilchenmann AG operates a redundant firewall infrastructure with a zone concept to secure each site. Partner access is provided through secured VPN connections. Data transfers occur via VPN or encrypted TLS/SSL connections to ensure tamper-proof communication.
Additional protection concepts are implemented for attack detection and prevention, unauthorised data transfers, and logging of security events.

3.1.4. Data Backup

Data backup is ensured through a backup and recovery concept. The concept defines intervals and retention periods for different data types based on their sensitivity. The backup infrastructure and data backups are continuously monitored. Critical data is stored in a secure location to protect it from accidental destruction or loss.

3.1.5. Virus and Spam Protection

Kilchenmann uses technical protection measures (antivirus software, spam filters, spyware protection, and filters against unwanted websites) to prevent malfunctions and misuse of its IT resources.

3.2. Organisational Measures

3.2.1. Personnel

All employees of Kilchenmann AG are bound by contractually regulated confidentiality obligations. Information and data handling is regularly trained, ensuring high awareness in the use of communication tools. Participation in continuous cyber security awareness training is mandatory. Employees with administrative rights are subject to a separate administrator agreement.

3.2.2. Authentication

Access to workplace computers and individual applications is granted only via personal username and password. This allows traceability of access and data changes through logging. Multi-factor authentication is used to secure online resources and VPN access.

3.2.3. Authorisation

Access is defined through a rights and role concept. Employees have access only to systems and directories required for their specific tasks. Definitions and change requests are handled at department management level and follow the principle of separation of duties.
Administrative tasks at domain level follow the four-eyes principle and are logged in an immutable manner for traceability.

3.2.4. Partners and Subcontractors

Partners and subcontractors authorised to handle personal data are contractually required to comply with these standards.

3.2.5. Certification and Audits

The headquarters and branches of Kilchenmann AG are certified by the Swiss Association for Quality and Management Systems (SQS) according to ISO 9001:2015.
In addition, an annual internal audit is conducted by trained auditors under the supervision of the Quality Management department to improve quality and verify compliance with processes and guidelines.
Comprehensive testing of IT systems and networks is carried out at regular intervals through penetration tests performed by specialised providers.

3.2.6. Employee Training

As part of a continuous awareness campaign conducted annually, all employees receive extensive training and testing on various aspects of cyber security. A phishing email campaign is also carried out to further increase employee awareness.