80 YEARS: QUALITY
MADE IN GERMANY

As of 12.02.2026

Description of Technical and Organizational Measures (TOMs)

of the organization: HEINE Optotechnik GmbH & Co. KG

Note
General Equal Treatment Act (AGG) For reasons of easier readability, this document does not differentiate between gender. Corresponding terms apply to all genders in the sense of equal treatment.

Contents

1 Introduction

Data security is an important integrated part of data protection. Data security regulates the technical and organizational measures necessary to ensure the protection of personal data in the event of automated processing, i.e. in systems or programs.

If processors are involved, they must also be checked for compliance with data security (Art. 28 GDPR).

The European General Data Protection Regulation (GDPR) contains requirements in Art. 32 (1) GDPR that personal data must be processed securely using adequate technical and organizational measures. The implementation of the protection objectives (= measures) is left to the controller*, "taking into account the state of the art, the implementation costs and the type, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons"* (Art. 32 GDPR).

In assessing the adequate level of protection, particular account shall be taken of the risks associated with the processing, in particular through destruction, loss or alteration, whether accidental or unlawful, or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

For automated processing (i.e. mainly by hardware and software), the GDPR specifies various control areas, each of which contains different sub-points:

1. Pseudonymization and encryption wherever possible
2. Confidentiality
3. Integrity
4. Availability and resilience
5. Procedures for periodic review, evaluation and evaluation

For non-automated processing of personal data, the above-mentioned control areas are not directly applicable according to the wording of the law. However, for the best possible protection, it is recommended to organize data security based on the control areas in these cases as well.

2 Organizational matters

This ensures written documentation of the current level of data protection and provides employees with written guidelines in the form of work instructions, guidelines and leaflets for compliance. The employees employed in data processing are obliged to maintain confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b), 29, 32 para. 4 GDPR.

Some safeguards in the following checklist relating to this area are not separately disclosed, either because they are the responsibility of processors and are therefore regulated and audited separately, or because not all details should be published for reasons of confidentiality.

3 Security measures

The following points describe the technical and organizational measures operated by the organization.

3.1 Pseudonymization and encryption (Art. 32 para. 1 lit. a) GDPR)

Wherever possible, personal data is processed exclusively in pseudonymized form (i.e. without direct recognition of a data subject). In addition, wherever possible, data should only be sent or stored in encrypted form. The principle of proportionality applies here.

3.2 Confidentiality (Art. 32 para. 1 lit. b) GDPR)

3.2.1 Access control

Access control includes measures that are suitable for denying unauthorised persons access to data processing systems with which personal data is processed or used:

Measures
There are automatic access control systems at the site to monitor the entry into the building.
It is a fenced property.
There is a building security concept that addresses the access options.

The distribution rooms or areas of the building technology are secured against unauthorized access.
There are security measures against robberies.
There are appropriate, non-mechanical access controls to the building.
There is an obligation to wear company or company ID cards.
There is an obligation for strangers to identify themselves by means of visibly worn identification.
The company servers are operated in a closed and access-secured room.
The network components are located in designated access-controlled rooms.
The management and maintenance of the mechanical access control systems is regulated and documented.
Security zones are described in the building security concept.
The building security concept provides for safety zones of different classification and sensitivity.
A locking plan is available for all keys or other means of identification.
The production, storage, management and issuance of keys or other means of identification is centrally regulated and documented.
Only authorized persons have access to the server room.
Measures have been taken to monitor the space of the server room.
There are regulations for the access of external forces to the server room.

3.2.2 Access control

Measures that are suitable to prevent data processing systems from being used by unauthorised persons:

Measures
For all information systems and services, there is a formal user registration and deregistration for the assignment and withdrawal of access authorizations.
It is ensured that users only have access to the network services that they are expressly authorized to use.
It is ensured that only authorized persons have logical access to the network components.
There is a formal approval procedure that systems and applications with personal data have to go through before they are allowed to gain network access.
It is ensured that only authorized devices from private individuals or visitors have logical access to the organization's network.
The Wi-Fi is secured against unauthorized access.
At regular intervals, independent testers simulate an attack on the network to identify vulnerabilities.
Software changes during maintenance assignments are monitored.
There are measures for the identification and authentication of external maintenance personnel.
Local maintenance by external parties ensures that no equipment can leave the data processing area unchecked.
With remote maintenance, the connection is established by a person who is a member of their own organization.
The connection is established from within the network.

3.2.3 Access control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be

read, copied, altered or removed without authorisation during processing, use and after storage.

Measures
Software changes during maintenance assignments are monitored.
The principle of the tidy desk and the blank screen is lived (Clean Desk Policy).
There are instructions that computer equipment (PC, laptop, smartphone, etc.) is sufficiently protected (e.g. by logging out of the system, etc.) when unattended.
There are instructions on how to deal with data carriers that are no longer needed (including written or printed paper).
The data on PCs and laptops is encrypted.
BitLocker is used so that it can be assumed that encryption algorithms and key lengths are sufficiently secure.
The disposal or reuse of devices equipped with storage media is regulated.
It is ensured that documents and data carriers whose retention period expires are permanently destroyed or deleted.
Special security software is used to ensure data security and access security.

3.2.4 Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.

Measures
Personal data on the systems are physically separated from each other (processing of different data sets on separate systems).

Personal data on the systems are logically separated from each other (different data records in a uniform database are marked according to their purpose (software-based distinctiveness)).
The systems used in the company are multi-client capable.
The multi-client capacity for the proceedings affected by this has been implemented throughout.
Office, development, test and action systems are located in clearly separated network segments, where possible even physically separated from each other.

3.2.5 Pseudonymization

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures.

Measures
Pseudonymization procedures in the company are used with separate storage of the assignment file.

3.3 Integrity (Art. 32 para. 1 lit. b) GDPR)

3.3.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers, and that it is possible to check and determine to which entities the transfer of personal data by means of data transmission is envisaged.

Measures
All persons involved in the processing/use of personal data are obliged to maintain confidentiality.
All new employees are given information on data protection as part of the confidentiality obligation.
Employees who process/use personal data are trained in data protection in the workplace in accordance with data protection regulations.
There is a process for departing employees, especially those who have been terminated.
There is a company-wide scheme for classifying data.
Appropriate security measures for the physical transport of data carriers (including paper) have been implemented.
It is ensured that data is transmitted only to the addressees specified by the Client or to the correct addressees according to the intended purpose.
The program-controlled transmissions are logged by recording the calling procedure, receiver, data, time.
The transmission of passed on data is encrypted.
When passing on data, the possibilities of anonymization/pseudonymization are used as far as possible.
Appropriate measures ensure that it is not possible or very difficult to uncover the pseudonym.

3.3.2 Input control

Measures to ensure that it is possible to verify and determine retrospectively whether and by whom personal data has been entered, altered or removed from data processing systems.

Measures
System usages are logged.
It is documented which user- or process-related evaluation options are used in the company.
It is known (and documented) which tools (audit programs) are used for the automatic evaluation of log files and which filter criteria are applied.
The logged data is subject to a strict purpose.
The logged data is protected against unauthorized access or manipulation.
An IT security officer has been appointed.

3.4 Availability and resilience (Art. 32 para. 1 lit. b) and c) GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss and can be quickly restored in the event of a physical or technical incident.

Measures
A risk and vulnerability analysis was carried out.
The risk factors against the maintenance of IT operations were examined.
An emergency manual exists and is constantly updated.
Responsibility and authority to issue instructions in the event of a disaster are clearly regulated.
The systems are protected against failure.
At regular intervals, it is checked whether the supply of telecommunications and data lines, electricity, heat and water is still sufficient.

The supply lines run underground.
Complete documentation of the air conditioning technology used is available.
Sufficiently dimensioned UPSs are used.
The UPS is designed for a supply time of 40 minutes.
Constant monitoring of the output voltage(s) takes place.
The UPS system has surge protection devices.
There are lightning protection devices.
There are no flammable items in the server area.
An early warning system with automatic fire detectors has been installed.
The fire alarm system is regularly maintained.
Push-button detectors for manual alarm triggering are available and clearly marked.
Alarm messages from the early warning system are passed on.
Regular maintenance and inspection of the smoke detectors and manual fire extinguishers takes place.
There is a written document for the IT restart (composition and tasks of the disaster management team).
There is an emergency concept for the network.
Regular backups are performed.
The requirements for the backup are documented in a backup concept.
Regular backups are performed.
The backups are encrypted.
The backups are protected from theft and destruction.

The processes for securing were created and documented in instructions.
The persons responsible for securing the security were named and documented.
It is regularly tested whether the backup is usable.
There is a written document for the computer restart.
There is a separate archive room.
There is a safety archive in another building or fire compartment.
Access to the archive is limited to a precisely defined group of people.
There is an emergency power shutdown.
There is a sensible division into fire compartments.
Compliance with air temperature and humidity is monitored.
Alarm and fire protection exercises are carried out.
Penetration tests are carried out.
Antivirus software is used.
An IDS (intrusion detection system) or IPS (intrusion prevention system) is used.

3.5 Procedures for regular review, assessment and evaluation (Art. 25 para. 1 GDPR; Art. 32 para. 1 lit. d) GDPR)

3.5.1 Organizational Security Criteria

Organizational security describes all organizational measures (instructions, procedures, etc.) to ensure and improve security.

Measures	Note
A data protection management system (DSMS) has been introduced and contains the most important data protection requirements and a comprehensive structure for mapping data protection measures.	
Incident response management is in place.	
Regular IT security audits are carried out.	
Regular education and sensitization of employees and managers are carried out.	

3.5.2 Order control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the instructions of the client.

Employees who have access to the systems as administrators are all instructed in data protection, obliged to maintain confidentiality and have accepted corresponding confidentiality and non-disclosure agreements as part of their employment contract.

If it uses processors for data processing, certain specifications will be implemented. This includes ensuring the technical and organisational measures of the contractors within the meaning of Art. 28 GDPR and Art. 32 para. 1 GDPR.

The prerequisite for entering into order processing is basically a legal basis. For a contract for commissioned data processing in accordance with Art. 28 para. 3 GDPR, all required measures and specifications must be complied with.

Measures
All processors are fully contractually obligated.
All order processing agreements have been checked in accordance with data protection law.