Description of technical and organisational measures (TOMs)

for the organisation: HEINE Optotechnik GmbH & Co. KG

Reviewer: Kaiyi Lin

Changes and approvals				
Prepared by: Erika Girg-Preiherr, Nicole Frister, Kaiyi Lin				
Version	Date	Responsible	Change	Review
1.0	07.10.2020			Kaiyi Lin
2.0	20.12.2021			Kaiyi Lin
	[Enter date]			
	[Enter date]			

Note
General Equal Treatment Act (AGG) For ease of reading, this document makes no gender-specific distinctions. Relevant terms are to be interpreted in a gender-neutral way for all genders.

4.1 Data security: Description of TOMs

Technical and organisational measures in accordance with Art. 32 para. 1 GDPR

Contents

4.1 Data security: Description of TOMs

Technical and organisational measures in accordance with Art. 32 para. 1 GDPR

1 Introduction

Data security is an important, integral part of data protection. Data security is governed by the technical and organisational measures that are required to ensure the protection of personal data in automated processing, such as in systems or programs.

If order processors are involved, these parties must also be verified as compliant with data security (Art. 28 GDPR).

Art. 32 para. 1 of the European General Data Protection Regulation (GDPR) includes provisions that personal data must be processed securely using adequate technical and organisational measures. Implementation of the protection objectives (= measures) is the responsibility of the controller*, "taking account of the status of the technology, the implementation costs and the type, scope, circumstances and purpose of processing, as well as the various probabilities and severities of risks for the rights and liberties of natural persons"* (Art. 32 GDPR).

In assessing the appropriate level of protection, consideration must be given to the risks associated with processing – in particular, through destruction, loss or alteration, whether accidental or unlawful, or unauthorised disclosure of, or unauthorised access to, personal data that has been transmitted, stored or processed in some other way.

For automated processing (i.e. particularly by hardware and software), the GDPR includes various control sections that each include various subsections:

(1) Pseudonymisation and encryption whenever possible
(2) Confidentiality
(3) Integrity
(4) Availability and capacity
(5) Procedures for regular review, assessment and evaluation

The aforementioned control sections do not apply directly, according to the wording of the law, for non-automated processing of personal data. However, even in these cases, to ensure the best possible protection of data, data security in line with these control sections is recommended.

2 Organisational

These measures ensure the written documentation of the current level of data protection and provide employees with written provisions in the form of work instructions, guidelines and fact sheets with which they must comply. People employed in data processing are obliged to ensure data confidentiality in accordance with Art. 28 para. 3 S 2b), 29, 32 para. 4 GDPR.

Some security measures in the checklist below concerning this section are not listed separately, as they either fall within the responsibility of order processors and are thus separately governed and checked, or because not all details can be published for reasons of confidentiality.

3 Security measures

The following points detail technical and organisational measures implemented by the organisation.

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

Whenever possible, personal data is only processed when it is pseudonymised (thus making it impossible to directly identify a data subject). Whenever possible, data should also be transmitted or stored only when encrypted. The principle of proportionality is applicable here.

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

3.2.1 Admission control

Admission control includes measures designed to deny unauthorised admission to data processing facilities that are used to utilise or process personal data.

Measures
This is a description of all admission control measures used on site.
The site is completely enclosed.
There are security measures against raids.
There are appropriate non-machine-based access controls to the building.
There is an obligation to wear company or service provider ID.
Visitors are required to wear an ID badge where it is clearly visible.
The company's servers are housed in a locked and secured room.
Network components are located in the appropriate admission-controlled rooms.

3.2.2 System access control

System access control measures are designed to avoid the unauthorised use of data processing systems.

Measures
There is a formal user registration and deregistration process for all information systems and services for the assignment and withdrawal of system access authorisations.
Users are only given access to network services for the purposes for which they are expressly authorised.
Only authorised people have logical access to network components.
There is a formal approval procedure that systems and applications with personal data have to go through before network access can be granted.
Only authorised devices of private individuals or visitors are given logical access to the organisation's network.

The WLAN is secured against unauthorised access.
There are measures in place for the identification and authentication of external maintenance personnel.
For local maintenance by external parties, no items of equipment can leave the data processing area unchecked.
For remote maintenance, a connection is set up by a person who is a member of the own organisation.
Connections are established from within the network.
The security measures arranged for system access control are tested on a regular basis to establish whether they continue to fulfil the required protective purpose.

3.2.3 Data access control

Data access control measures ensure that only the persons authorised to use a data processing system may access the data they are allowed to access and that, when personal data is processed, used and after it is stored, there is no unauthorised reading, copying, amendment or deletion.

Measures
A clean desk and blank screen policy apply.
There are instructions that data-processing equipment (PC, laptop, smartphone, etc.), if left unattended, should be adequately protected (e.g. by logging off the system, etc.).
There are instructions on how to deal with media that is no longer required (including handwritten or printed paper documents).
Data on PCs and laptops is encrypted.
BitLocker is used so that adequate secure encryption algorithms and key lengths can be assumed.
There are rules for the disposal or re-use of devices equipped with storage media.
Documents and media whose retention period has expired are destroyed or deleted in a sustainable manner.

3.2.4 Separation rule

These measures ensure that data gathered for various purposes can be separately processed.

Measures
There is physical separation of personal data on systems (processing of different data records on separate systems).
There is logical separation of personal data on systems (different data records in a single database are marked according to purpose (software distinguishability)).

The systems used in the organisation support multiple clients.
The multiple-client capability for the procedures concerned is consistently implemented.
Office, development, test and live systems are located in network segments that are clearly separate from each other; where possible, they are even physically separate from each other.

3.2.5 Pseudonymisation

The processing of personal data such that the data can no longer be assigned to a specific data subject without the inclusion of additional information, provided that this additional information is stored separately and subject to the relevant technical and organisational measures.

Measures
Pseudonymisation procedures in the organisation are applied with separate storage of the assignment file.

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

3.3.1 Forwarding control

Forwarding control measures ensure that when personal data is transferred electronically or whilst it is being transported or stored on media, it cannot be read, copied, amended or deleted without authorisation. These measures also ensure that it is possible to verify and determine the intended locations for the transmission of personal data by means of data transmission facilities.

Measures
All people employed in the processing/use of personal data are obliged to uphold the duty of confidentiality.
All new employees are issued with data protection information regarding this confidentiality obligation.
Employees who process/use personal data are trained through data protection training sessions on compliance with data protection conduct in the workplace.
There is a process for employees leaving the organisation, particularly those who are dismissed.
Appropriate security measures for the physical transport of media (including paper) are implemented.
These measures ensure that data is only transmitted to the correct addressees as specified by the principal or the intended purpose.
Forwarded data is encrypted when transmitted.
When forwarding data, anonymisation/pseudonymisation is used as far as possible.

3.3.2 Entry control

Entry control measures ensure it is subsequently possible to check and verify whether and by whom personal data has been entered, amended or deleted in data processing systems.

Measures
Logged data is subject to strict intended use rules.
Logged data is protected against unauthorised viewing or manipulation.

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

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

Measures
There is an emergency manual which is updated regularly.
There are clear rules regarding responsibility and authority in the event of a disaster.
Systems are protected against breakdown.
Checks are made at regular intervals to ensure there is always adequate provision of telephone lines and data cables, power, heat and water.
Supply cables and pipelines run underground.
A sufficiently dimensioned uninterrupted power supply (UPS) is used.
The UPS is designed to supply power for 40 minutes.
Output voltages are constantly monitored.
The UPS system has overvoltage protection.
There is lightning protection equipment.
No flammable items are located in the server area.
An early warning system with automatic fire alarms is installed.
The fire alarm system is maintained regularly.
Push-button alarms for activating the alarm manually are available and clearly labelled.

Alarm signals are relayed from the early warning system.
Smoke detectors and hand-held fire extinguishers are inspected and serviced regularly.
Backup requirements are documented in a backup plan.
Regular backups are carried out.
Backups are encrypted.
Backups are protected against theft and destruction.
The security processes have been created and documented in a set of guidelines.
The people responsible for security have been named and documented.
Regular tests are conducted to check that the backup is usable.
There is a written document for data processing recovery.
There is a separate archive room.
There is a security archive in a different building or fire area.
Access to the archive is restricted to a clearly defined group of people.
There is an emergency shut-off for the power supply.
The site is logically separated into fire areas.
Maintenance of the air temperature and humidity is monitored.
Antivirus software is used.
An IDS (intrusion detection system) or IPS (intrusion prevention system) is used.

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

3.5.1 Order control

Order control measures ensure that personal data processed under contract can only be processed in accordance with the principal's instructions.

4.1 Data security: Description of TOMs

Technical and organisational measures in accordance with Art. 32 para. 1 GDPR

Employees with administrator access to the systems are all trained in data protection, are obliged to maintain confidentiality and, as part of their employment contract, have accepted the corresponding confidentiality and secrecy agreements.

If order processors are used for data processing, specific provisions are implemented. These provisions include ensuring that the contractor has implemented technical-organisational measures according to Art. 28 GDPR and Art. 32 para. 1 GDPR.

The precondition for entering into order processing is, in principle, a legal basis. To conclude a contract for order data processing according to Art. 28 para. 3 GDPR, all required measures and provisions must be complied with.

Measures
All order processors are fully bound by contract.
All order processing contracts are checked to ensure they comply with data protection legislation.