Appendix 2 Data security: Description of TOMs

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

Description of technical and organisational measures (TOMs)

for the organisation:

SaSG GmbH & Co. KG

Changes and approvals				
Prepared by: Peter Heidenreich, Kaiyi Lin				
Version	Date	Responsible	Change	Review
1.0	22.01.2020			Kaiyi Lin

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.

Appendix 2 Data security: Description of TOMs

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

Contents

Appendix 2 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	Note
The site is equipped with automated admission control systems for monitoring access in and out of the building.	
The building is a stand-alone complex.	
The distribution rooms or areas of the building technology are secured against unauthorised access.	
There is continuous external perimeter security with measures to prevent break-ins.	
There are security measures against raids.	
The company's servers are housed in a locked and secured room.	

3.2.2 System access control

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

Measures	Note
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.	
Software changes during maintenance assignments are monitored.	

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	Note
Users ensure that their data processing equipment is adequately protected if left unattended.	
Users will see the time of the last procedure.	
There are rules for the disposal or re-use of devices equipped with storage media.	

3.2.4 Separation rule

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

Measures	Note
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.	

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	Note
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.	

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.	

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	Note
There are rules regarding how long this logged data should be retained.	
This 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	Note
The risk factors against the maintenance of the data processing operation have been assessed.	
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.	
There are no water pipes in computer rooms.	
A sufficiently dimensioned uninterrupted power supply (UPS) is used.	
The UPS is designed to supply power for 20 minutes.	
The UPS system has overvoltage protection.	
There is ightning protection equipment.	
No flammable items are located in the server area.	
An early warning system with automatic fire alarms is installed.	

There are sufficient numbers of appropriate fire extinguishers available with the right types of extinguishing agent; extinguisher provision and type is consistent across the site.	
There are backup computer centres/substitute computers/substitute rooms.	
There is a disaster recovery plan for the network.	
Regular backups are carried out.	
The media where backups are stored are encrypted.	
Backups are protected against theft and destruction.	
Backups are tested annually to check that they are usable.	
There is an emergency shut-off for the power supply.	
There is a substitute centre.	
Antivirus software is used.	

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

3.5.1 Organisational security criteria

Organisational security describes all organisational measures (guidelines, procedures, etc.) that ensure and improve security.

Measures	Note
Employees and management are regularly trained in and made aware of these measures.	
A data protection management system (DPMS) is implemented.	