List of technical organizational measures (TOM) within the meaning of Art. 32 GDPR

of the organization

Alarm IT Factory GmbH

As at: June 2023

Classification: External

Change history

Version	Date	Change	Author	Release by
1.0	22.06.2023	Document creation/translation	MB	
1.1	22.06.2023	Review and release	MB, STAR	DA

Organizations that collect, process or use personal data themselves or on behalf of others must take the technical and organizational measures required to ensure that the provisions of data protection laws are implemented. Measures are only necessary if their cost is in reasonable proportion to the intended protective purpose.

The above organization meets this requirement through the following measures:

1 Confidentiality according to Art. 32 para. 1 lit. GDPR

1.1 Physical access control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used. Access control measures that can be used to secure buildings and rooms include automatic access control systems, use of chip cards and transponders, control of access by gatekeeper services and alarm systems. Servers, telecommunications equipment, network technology and similar equipment should be protected in lockable server cabinets. In addition, it makes sense to support access control by organizational measures (e.g., instructions stipulating that offices be locked during absences).

Technical measures	Organizational measures
☒ Automatic access control system	☒ Key rules/list
☒ Chip cards/transponder systems	☒ Visitors accompanied by employees
☒ Doors with knob outside	☒ Care during the selection of cleaning services

1.2 Data access control

Measures suitable for preventing data processing systems (computers) from being used by unauthorized persons.

Data access control refers to the prevention of the use of equipment by unauthorized individuals. Possibilities include, for example, boot password, user ID with password for operating systems and software products used, screensaver with password, the use of chip cards for logging in as well as the use of call-back procedures. In addition, organizational measures may also be necessary, for example to prevent unauthorized viewing or inspection (e.g. specifications for setting up screens, issuing guidance for users on how to choose a "good" password).

Technical measures	Organizational measures
☒ Login with username + password	☒ Managing user permissions
☒ Anti-virus software server	☒ Creating user profiles
☒ Anti-virus software clients	☒ "Secure password" policy
☒ Firewall	☒ "Delete/Destroy" policy
☒ Intrusion detection systems	☒ "Clean desk" policy
☒ Use of VPN for remote access	☒ General guidelines on data protection and/or security
☒ Encryption of data carriers	☒ Mobile device policy
☒ Automatic desktop lock	☒ "Manual desktop lock" guide
☒ Encryption of notebooks/tablets	

1.3 Data usage control

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use and after storage. Data usage control can be ensured, among other things, by suitable authorization concepts that enable differentiated control of access to data. This involves differentiating both the content of the data and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined in order to document the granting and revocation of authorizations and to keep them up to date (e.g. in the event of hiring, change of job, termination of employment). Special attention must always be paid to the role and possibilities of the administrators.

Technical measures	Organizational measures
☒ File shredder (min. level 3, cross cut)	☒ Use of authorization concepts
	☒ Minimum number of administrators
	☒ Management of user rights by administrators

1.4 Separation control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical measures	Organizational measures
☒ Separation of production and test environment	

1.5 Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

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

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

2.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data carriers, and that it is possible to check and determine to which entities personal data is intended to be transmitted by data transmission equipment. Encryption techniques and virtual private networks, for example, can be used to ensure confidentiality during electronic data transmission. Measures for transporting or forwarding data carriers include transport containers with locking devices and regulations for destroying data carriers in accordance with data protection requirements.

Technical measures	Organizational measures
☒ E-mail encryption (possible upon customer request)	☒ Care in the selection of transport personnel and vehicles
☒ Use of VPN	☒ Requirements for transmission of information according to classification as per specific policy for this purpose

☒ Logging of access and retrieval	
☒ Provision via encrypted connections such as sftp, http	

2.2 Input control

Measures that ensure that it is possible to check and determine retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved by logging, which can take place at various levels (e.g. operating system, network, firewall, database, application). It must also be clarified which data is logged, who has access to logs, by whom and on what occasion/at what time these are checked, how long storage is required and when deletion of the logs takes place.

Technical measures	Organizational measures
☒ Technical logging of data input, modification and deletion	☒ Traceability of input, modification and deletion of data by individual usernames (not user groups)
☒ Manual or automated control of logs	☒ Assignment of rights to enter, change or delete data based on authorization concept

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

3.1 Availability control

Measures that ensure that personal data is protected against accidental destruction or loss. This involves topics such as an uninterruptible power supply, air-conditioning systems, fire protection, data backups, secure storage of data carriers, virus protection, raid systems, disk mirroring, etc.

Technical measures	Organizational measures
☒ Fire and smoke detection systems	☒ Backup & recovery concept (formulated)
☒ Fire extinguisher in server room	☒ Control of the backup process

☒ Server room monitoring, temperature and humidity	☒ Regular data recovery tests and logging of results
☒ Server room, air-conditioned	☒ Storing the backup media in a safe place outside the server room
☒ UPS	☒ No sanitary connections in or above the server room
☒ Protective socket strips in server room	☒ Existence of an emergency plan (e.g. BSI IT-Grundschutz 100-4) (baseline protection)
☒ RAID system/hard disk mirroring	☒ Separate partitions for operating systems and data

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

4.1 Data protection management

Technical measures	Organizational measures
☒ Central documentation of all procedures and regulations on data protection with access for employees according to need/authorization (e.g. wiki, Intranet, etc.)	☒ External data protection officer: Secopan GmbH datenschutz@secopan.de
☒ Other document security safety	☒ Employees trained and committed to confidentiality/data secrecy
☒ A review of the effectiveness of the technical protective measures is carried out at least once a year	☒ Regular training of employees to raise awareness. At least once a year
	☒ External information security officer: Secopan GmbH datenschutz@secopan.de

	☒ The Data Protection Impact Assessment (DPIA) is carried out as required
	☒ The organization complies with the information requirements according to Art. 13 and 14 GDPR
	☒ Formalized process for processing data subject access requests is in place

4.2 Incident response management

Support with security breach response.

Technical measures	Organizational measures
☒ Use of firewall and regular updating	☒ Documented process for detecting and reporting security incidents/data breaches (also with regard to reporting obligation to supervisory authority)
☒ Use of spam filters and regular updating	☒ Documented procedure for handing security incidents
☒ Use of virus scanners and regular updating	☒ Integration of ☒ data protection officer and ☒ information security officer in security incidents and data breaches
☒ Intrusion Detection System (IDS)	☒ Documentation of security incidents and data breaches, e.g. via ticket system
☒ Intrusion Prevention System (IPS)	☒ Formal process and responsibilities for the follow-up of security incidents and data breaches

4.3 Privacy-friendly default settings (Art. 25 para. 2 GDPR)

Privacy by design / Privacy by default

Technical measures	Organizational measures
☒ No more personal data is collected than is necessary for the respective purpose	

4.4 Order control (outsourcing to third parties)

Measures that ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions. In addition to data processing on behalf of the customer, this point also includes the performance of maintenance and system support work both on site and via remote maintenance. If the contractor uses service providers within the meaning of order processing, the following points must always be arranged with them.

Technical measures	Organizational measures
	☒ Prior review of the security measures taken by the contractor and their documentation
	☒ Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
	☒ Conclusion of the necessary order processing agreement or EU standard contractual clauses
	☒ Written instructions to the contractor
	☒ Obligation of the contractor's employees to maintain data secrecy (AVV/NDA) according to the specifications of the ISMS
	☒ Obligation to appoint a data protection officer by the

	contractor if there is an obligation to appoint one
	☒ Agreement on effective control rights vis-à-vis the contractor
	☒ Regulation on the use of further subcontractors
	☒ Ensuring the destruction of data after completion of the order
	☒ In case of longer cooperation: Ongoing review of the contractor and their level of protection

Completed for the organization by

Name	Davide Acquadro
Position	Managing Director

For Alarm IT Factory GmbH

Date: 22.06.2023