Technical und Organizational Measures (TOM)

As used in section 32, paragraph 1, sentence 1 lit. of the general data protection regulation (GDPR)

The organization:

Statista GmbH
Johannes-Brahms-Platz 1
20355 Hamburg

Status: June 2021

Organizations that collect, process, or use personal data themselves or on behalf of their respective organizations must take the technical and organizational measures necessary to ensure that data protection laws are implemented. Measures are only necessary if efforts are proportionate to the intended protected purpose.

The above-mentioned organization meets these demands through the following measures:

Confidentiality in section 32, paragraph 1, lit. GDPR

Entry control

Measures that are suitable for denying unauthorized persons access to data processing systems with which personal data is processed or used. Access control measures for buildings and room security include automatic access control systems, the use of chip cards and transponders, monitoring access through porter services, and the use of alarm systems. Servers, telecommunication systems, network technology, and similar systems must be protected in lockable server cabinets. In addition, it is sensible to support access control by means of organizational measures (for example, service instructions which provide for the closure of service rooms in the event of absence).

Technical measures		Organizational measures	
	Alarm system	X	Key schedule / list
X	Automated access control systems	X	Reception / doorman
	Biometric entry barriers		Visitor's book / visitor log
X	Chipcards / transponder system	X	Employee / visitor passes
X	Manual locking system		Visitors accompanied by employees
X	Security locks (server rooms)		Careful selection of transport personnel and vehicles
	Locking system with a code lock	X	Careful selection of cleaning services
X	Safeguarding of building shafts		
X	Doors with the knob on the outside		
	Bell system with a camera (currently disabled)		
	Video surveillance of the entryway		

Admission control

Measures that are suitable for preventing data processing systems (computers) from being used by unauthorized persons. Admission control refers to the unauthorized prevention of the use of equipment. Options include a boot password, a user ID with a password for operating systems and used software products, a screensaver with a password, using chip cards for logging in, as well as using callback procedures. In addition, organizational measures can also be necessary to prevent inspection by unauthorized persons (for example, guidelines for setting up screens, providing guidelines to users on how to choose a "good" password).

Technical measures		Organizational measures	
X	Login with username + password	X	Managing user privileges
	Login with biometric data	X	Creating user profiles
X	Anti-virus software server	X	Centrally assigning passwords
X	Anti-virus software client	X	Guideline “secure password”
	Anti-virus software mobile devices		Guideline “delete / erase”
X	Firewall	X	Guideline “clean desk” (not in other areas)
X	Intrusion detection system	X	General data protection / security policy

	Mobile device management		Mobile device policy
X	Use of VPN for remote access	X	Guideline “manual desktop lock”
X	Encryption from data carriers		
X	Encryption smartphones		
	Housing lock		
X	BIOS protection (separate password)		
	Blocking of external interfaces (USB)		
X	Automatic desktop lock		
X	Encryption from notebooks / tablets		

Further measures:

Access control

Measures to 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, changed, or removed without authorization during processing, use, and after storage. Access control can, among other things, be guaranteed by suitable authorization concepts that enable differentiated control of access to data. It is important to differentiate between the data content and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined to document the assignment and withdrawal of authorizations and to keep them up to date (e.g., when hiring, changing jobs, or terminating employment). Particular attention should always be paid to the roles and possibilities of the administrators.

Technical measures		**Organizational measures**	
	File shredder (at least level 3, crosscut)	X	Use of authorization concepts
X	External file shredder (DIN 32757)	X	Minimum number of administrators
X	Physical deletion of data carriers	X	Data protection vault (will be implemented at short notice)

X	Logging (depending on the system)	X	Administration of user rights by administrators

Further measures:

Separation control

Measures to 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**	
X	Separation of productive and test environment	X	Control over authorization concept
X	Physical separation (systems / databases / data carriers)	X	Definition of database rights
X	Multi-client capability of relevant applications	X	Data records are provided with purpose attributes

Further measures:

Pseudonymization (section 32, paragraph 1, lit. a GDPR, section 25, paragraph 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 the use of additional information; provided that such additional information is kept separately and is subject to appropriate technical and organizational measures;

Technical measures		Organizational measures	
	In the case of pseudonymization: Separation of the assignment data and storage in a separate and secure system (possibly encrypted)	X	Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or after the statutory deletion period has expired

Further measures:

Integrity (section 32, paragraph 1, lit. b GDPR)

Data transfer control

Measures to ensure that personal data cannot be read, copied, changed, or removed without authorization when transferring electronically, or when transporting or storing on data carriers. These measures can also be verified and established where the transfer of personal data through data communication equipment is provided. To ensure confidentiality of electronic data transfers, for example with encryption techniques and a virtual private network. Measures for data carrier transportation, or data transmission are transportation containers with a locking device and regulations for data protection-compliant destruction of data carriers.

Technical measures		Organizational measures	
	Email encryption		Documentation of the data recipients as well as the duration of the planned release or deletion periods
X	Using a VPN	X	Documentation of the data recipients as well as the duration of the planned release or deletion periods
	Personal handover with a protocol		Disclosure in anonymous or pseudonymous form
X	Safe transport containers (via Reisswolf)	X	Careful selection of transport personnel and vehicles
X	Provision via encrypted connections such as sftp, https		Personal handover with a protocol
	Use of signature methods		

Further measures:

Input control

Measures to ensure that it can subsequently be verified and ascertained whether and by whom personal data has been entered, altered, or removed in data processing systems. Input control is achieved through logging that can take place at different levels (e.g., operating system, network, firewall, database, application). It is also necessary to clarify which data is logged, who has access to logs, by whom and at what occasion/time they are controlled, how long retaining records is required, and when deleting the records takes place.

Technical measures		**Organizational measures**	
X	Technical logging of the entry, modification, and deletion of data		Overview of which programs can be used to enter or delete which data
	Manual or automated control of protocols	X	Traceability of input, modification, and deletion of data by individual usernames (not user groups)
		X	Granting rights to enter, change and delete data based on an authorization concept
		X	Storage of forms from which data has been transferred to automated processing

Further measures:

Availability and capacity (section 32, paragraph 1, lit, b. GDPR)

Availability controls

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

Technical measures		**Organizational measures**	
X	Fire and smoke alarm systems		Backup & recovery concepts (formulated)
X	Fire extinguisher in the server room	X	Monitoring the backup process
X	Monitoring the server room's temperature and humidity		Regular tests for data recovery and logging results
X	Air-conditioned server room	X	Storing backup media in a secure location outside the server room
X	USV	X	No sanitary facilities in or above the server room
X	Protective socket strips in the server room		Having an emergency plan (e.g., BSI IT-basic protection 100-4
X	Data protection safe (S60DIS, S120DIS, other suitable standards with source seal etc.	X	Data protection safe (S60DIS, S120DIS, other suitable standards with source seal etc
X	RAID system / disk mirroring		
X	Server room with CCTV		
	Alarm notification in the case of unauthorized access		

Further measures:

Procedure for a regular review, assessment, and evaluation (section 32, paragraph 1, lit. D GDPR; section 25, paragraph 1 GDPR)

Data protection management

Technical measures		Organizational measures	
X	Software solutions for data protection management in operation	X	Internal data protection officer name / company / contact details
X	Central documentation of all procedures and regulations for data protection with access facilities for employees as required/authorized (e.g., wiki, intranet…)	X	Employees trained and bound to confidentiality / data secrecy
	Security certification in accordance with ISO 27001, BSI baseline protection or ISIS12	X	Regularly raising awareness among employees on at least a yearly basis
X	Other documented security concept		Internal / external information security officer / name / company / contact
X	A review of the effectiveness of the technical protection measures shall be carried out at least annually	X	The Data Protection Impact Assessment (DSFA) is carried out if necessary
		X	The organization follows the information obligations under Articles 13 and 14 DSGVO
		X	A formalized process for handling enquires for those concerned is in place

Further measures:

Incident response management

Assistance in responding to security breaches

<table>
<tr><th colspan="2">Technical measures</th><th colspan="6">Organizational measures</th></tr>
<tr><td>X</td><td>Use of firewall and regular updates</td><td>X</td><td colspan="5">Documented process for the detection and reporting of security incidents / data breaches (also with regards to the reporting to the supervisory authority)</td></tr>
<tr><td>X</td><td>Use of spam filters and regular updates</td><td></td><td colspan="5">Documented approach for dealing with security incidents</td></tr>
<tr><td>X</td><td>Use of virus scanners and regular updates</td><td>X</td><td>Integration of security incidents and data breaches</td><td>X</td><td>DPO</td><td></td><td>ISO</td></tr>
<tr><td>X</td><td>Intrusion detection system (IDS)</td><td>X</td><td colspan="5">Documentation of security incidents and data breaches e.g., via the ticket system</td></tr>
<tr><td>X</td><td>Intrusion prevention system (IPS)</td><td>X</td><td colspan="5">Formal process of responsibilities for post-processing security incidents and data breaches</td></tr>
</table>

Further measures:

Data protection friendly default settings (section 25, paragraph 2, GDPR);

Privacy by design / Privacy by default

Technical measures		Organizational measures	
X	No more personal data is collected than necessary for the respective purpose	X	Double opt-in procedure
X	Simple exercise of the data subject's right of withdrawal via technical activities		

Further measures:

Order control (outsourcing to third parties)

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with their instructions. In addition to data, this includes the execution of maintenance and system support work both on site and via remote maintenance. Provided that the contractor uses service providers for order processing, the following points must always be regulated with them.

Technical measures		**Organizational measures**	
		X	Prior investigation of the security measures taken by the contractor and their documentation
		X	Choosing the contractor based on due diligence points (especially with regard to data protection and data security)
			Conclusion of the necessary contract processing agreement or EU standard contractual clauses
		X	Written instructions to the contractor
		X	Commitment of the contractor's employees to data secrecy
		X	Obligation to appoint a data protection officer by the contractor if required by the contractor
			Agreement of effective control rights vis-à-vis the contractor
			Regulation on the use of additional subcontractors
			Ensuring the destruction of data after completion of the order
		X	In case of prolonged cooperation: Ongoing review of the contractor and his level of protection

Further measures:

Completed for the organization by:

Name: Christian Wolf
Function: Data protection officer

Contact number: +49 40 284 841 679
Email: Christian.Wolf@Statista.com

To be filled in by the customer:

Examined on (date) by (name) . Result(s):

□ Further need for clarification

□ TOMs are sufficient for the desired purpose

□ An agreement for data processing can be made

Note: This template may still use terms from the older version of the German federal data protection act. In terms of content, the technical and organizational measures do not differ from those required by the GDPR!