

Technical and Organizational Measures (TOM)

Pursuant to Art. 32 GDPR

The organization:

Statista GmbH
Johannes-Brahms-Platz 1
20355 Hamburg

As of: November 2025

Organizations that collect, process, or store personal data, either as a controller or on behalf of another organization, must implement the technical and organizational measures required to ensure compliance with applicable data protection laws. Measures are only necessary if efforts are proportionate to the intended protective purpose.

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

Confidentiality in accordance with Art. 32 para. 1 lit. b GDPR

Physical access Control

Measures that are suitable for denying unauthorized persons access to data processing systems with which personal data are processed or used. Measures for access control to secure buildings and rooms include automatic access control systems, the use of chip cards and transponders, access control by gatekeeper services, and alarm systems. Servers, telecommunications systems, network technology, and similar systems must be protected in lockable server cabinets. In addition, it is sensible to support access control with organizational measures (e.g. service instructions that require offices to be locked in the event of absence).

Technical measures		Organizational measures	
x	Alarm system	x	Key regulation / list
x	Automatic access control system	x	Reception / doorman
	Biometric access barriers	x	Visitors' book / visitors' log
x	Chip Cards / Transponder Systems	x	Employee / visitor badges
x	Manual locking system	x	Visitors accompanied by employees
x	Security locks		Careful selection of building security staff
	Locking system with code lock	x	Careful selection of cleaning services

x	Securing the building shafts		
x	Doors with knob on the outside		
	Bell system with camera		
	Video surveillance of the entrances		

Authentication control

Measures that are suitable to prevent data processing systems (computers) from being used by unauthorized persons. Access control refers to the unauthorized prevention of the use of systems. Possibilities include boot password, user IDs with password for operating systems and software products, password-protected screen savers, the use of chip cards for login as well as the use of call-back procedures. In addition, organizational measures may also be necessary to prevent unauthorized access (e.g. guidelines for setting up screens, issuing guidance for 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	Central password assignment
x	Anti-Virus software clients	x	Strong Password policy
x	Anti-Virus software mobile devices	x	Delete/destroy policy
x	Firewall	x	Clean desk policy
x	Intrusion detection system	x	General data protection / security policy
	Mobile device management	x	Mobile device policy
x	Use of VPN for remote access	x	Guideline "Manual Desktop Lock"
x	Encryption of data carriers		
x	Encryption smartphones		
	Housing lock		
x	BIOS protection (separate password)		
	External interface lock (USB)		
x	Automatic desktop lock		
x	Encryption of notebooks / tablets		
x	Web application firewall (WAF)		

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, modified or removed without authorization during processing, use and after storage. Access control can be guaranteed, among other things, by suitable authorization concepts that enable differentiated control of access to data. It is important to differentiate between 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 assignment and withdrawal of authorizations and to keep them up to date (e.g., in the event of hiring, change of roles, terminating employment). Particular attention must always be paid to the roles and possibilities of the administrators.

Technical measures		Organizational measures	
	File shredder (at least level 3, cross cut)	x	Use of authorization concepts
x	External document shredder (DIN 32757)	x	Minimum number of administrators
x	Physical deletion of data carriers	x	Privacy Vault
x	Logging of access to applications, specifically when entering, modifying and deleting data	x	Management of user rights by Administrators
		x	Assignment of rights according to the principle of least privilege and functional separation (Segregation of Duties)
		x	Recertification of rights

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 production and test environment	x	Control via authorization concept
x	Logical separation of user data (e.g., through authorization concepts and multi-tenancy)	x	Definition of database rights
x	Processing of other personal data in separate internal systems (e.g., HR, Finance)	x	Records are tagged with purpose attributes.

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

Processing 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 separate and secured system (possibly encrypted)	x	Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or after the expiry of the statutory deletion period

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

Data Transfer control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during transport or storage on data carriers, and

that it is possible to verify and determine to which locations personal data is to be transmitted by means of data transfer. To ensure confidentiality in electronic data transfers, e.g., encryption techniques and virtual private networks can be used. Measures for the transport of data carriers or data transfer include transport containers with a locking device and regulations for the destruction of data carriers in accordance with data protection regulations.

Technical measures		Organizational measures	
x	Email encryption	x	Documentation of the data recipients and the duration of the planned transfer or deletion periods
x	Use of VPN	x	Overview of regular retrieval and transmission processes
x	Logging of accesses and retrievals		Disclosure in anonymized or pseudonymized 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 protocol
x	Use of digital signature mechanisms		

Input control

Measures to ensure that it is possible to verify and determine retrospectively whether and by whom personal data has been entered, modified or removed from data processing systems. Input control is achieved through logging, which can take place at different levels (e.g. operating system, network, firewall, database, application). It also needs to be clarified which data is logged, who has access to logs, by whom and on what occasion/time they are controlled, how long retention is required and when the logs are deleted.

Technical measures		Organizational measures	
x	Technical logging of data entry, modification, and deletion	x	Overview of which programs can be used to enter or delete which data
x	Manual or automated control of protocols	x	Traceability of input, modification and deletion of data by individual user names (not user groups)
		x	Retention of forms from which data has been transferred to automated processing
		x	Assignment of rights to enter, change and delete data on the basis of an authorization concept
		x	Clear responsibilities for deletions

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

Availability controls

Measures to ensure that personal data is protected against accidental destruction or

loss. This involves 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	x	Backup & Recovery concept
x	Fire extinguisher in the server room	x	Control of the backup process
x	Monitoring the server room's temperature and humidity	x	Regular tests for data recovery and logging of results
x	Air-conditioned server room	x	Storage of backup media in a secure location outside the server room
x	UPS	x	No sanitary facilities in or above the server room
x	Protective socket strips in the server room	x	Existence of an emergency plan
x	Data protection safe (S60DIS, S120DIS, other suitable standards with source seal, etc.)	x	Separate partitions for operating systems and files
x	RAID system / disk mirroring		
x	Server room with CCTV		
x	Cloud security posture management		

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

Data protection management

Technical measures		Organizational measures	
x	Software solutions for data protection management in operation	x	External Data Protection Officer
x	Central documentation of all procedures and regulations for data protection with access for employees as required / authorized (e.g. wiki, intranet ...)	x	Employees trained and committed to confidentiality/data secrecy
	Security certification in accordance to ISO 27001, BSI IT-Grundschutz, CISIS12 or similar	x	Regular awareness raising of employees at least once a year
x	Other documented security concept	x	Internal Information Security Officer
x	A review of the effectiveness of the technical protective measures shall be carried out at least annually	x	The Data Protection Impact Assessment (DPIA) is carried out if necessary
		x	The organization complies with the information obligations pursuant to Art. 13 and 14 GDPR
		x	A formalized process for processing requests for information from data subjects is in place
		x	Phishing simulations and security trainings

Incident-Response-Management

Assistance in responding to security breaches

Technical measures		Organizational measures	
x	Use of firewall and regular updates	x	Documented process for detection and reporting of security incidents / data breaches (also with regard to the reporting obligation to the supervisory authority)
x	Use of spam filters and regular updates	x	Documented procedure for dealing with security incidents
x	Use of virus scanner and regular updates	x	Involvement of DPOs and ISO in security incidents and data breaches
x	Intrusion detection system (IDS)	x	Documentation of security incidents and data breaches, e.g. via ticket system
x	Intrusion prevention system (IPS)	x	Formal process of responsibilities to follow up on security incidents and data breaches
x	Endpoint detection & response as well as central security monitoring	x	Incident runbooks
		x	24x7 security operations center (SOC)
		x	Regular vulnerability scans and annual external penetration tests

Privacy-friendly default settings (Art. 25 para. 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 measures		

Use and Control of External Service Providers

Measures ensuring that personal data processed in the context of cooperation with external service providers is processed strictly in accordance with contractual agreements and applicable legal requirements. This includes, in particular, activities such as maintenance and system support, both on-site and via remote access. When external companies are engaged to provide services, the Controller ensures that these entities implement appropriate technical and organizational measures to safeguard personal data.

Technical measures		Organizational measures	
x	Regulation and logging of access to systems (e.g., during maintenance, support, remote access)	x	Prior review and documentation of the security measures implemented by the service provider (including processors)

x	Use of secure remote access procedures	x	Careful selection of the service provider, particularly with regard to data protection and information security
x	Ensuring that maintenance activities are performed only when authorized and controlled	x	Conclusion of necessary agreements (e.g., Data Processing Agreement or EU Standard Contractual Clauses, where required)
		x	Definition of contractual requirements regarding data protection, confidentiality, and technical and organizational measures
		x	Ensuring the service provider's obligation to maintain confidentiality for its employees
		x	Agreement on effective audit and control rights toward the service provider
		x	Regulation of the use of additional subcontractors
		x	Obligation to delete or return personal data in a data protection-compliant manner at the end of the engagement
		x	Regular review of the service provider and its security level during long-term engagements