

Technical and organisational measures (TOM)



DealerCenter Digital GmbH

Ludwig-Erhard-Straße 13a
84034 Landshut

Data protection officer

Süddeutsche Datenschutzgesellschaft mbH
Am Pfaffensteiner Hang 17
93059 Regensburg

Phone: +49 941-38177070

Version	2.0
Date	08.10.2025
Status	intermediate inspection

The inspection was conducted in a videocall and was not verified on site. Completed on 08/10/2025 with the support of:

Name: Alexander Vetter
Position: CTO
E-mail address: alexander.vetter@bike.center

1. Confidentiality according to Art. 32 para. 1 (b) GDPR

1.1. Admission control

Admission control describes measures that prevent unauthorised persons from gaining access to processing systems with which data processing is carried out.

Technical measures

- Chip cards/transponders
- Manual or mechatronic locking system
- Workplace computers are in locked rooms
- Secured building shafts for basement rooms
- No external windows in the data centre and server room
- Sturdy, burglar-resistant or barred windows and doors on the ground floor (e.g. in accordance with DIN EN 1627)
- Measures to prevent easy eavesdropping and viewing (especially for customer reception, shared spaces or mobile working)
- Automatic locking of the end device after a certain period of inactivity (screen lock)
- BIOS protection
- Deactivation of unused network sockets

Organisational measures

- Documented key management
- Door locking rules
- Practised regulations for the access of external persons (e.g. escorts, access bans, ID cards)

1.2. Data carrier and memory control

Data carrier control describes measures that prevent the unauthorised reading, copying, modification or deletion of data carriers. Storage control describes measures to prevent the unauthorised input, access, modification and deletion of stored personal data.

Technical measures

- Mobile workstations (e.g. company notebooks, company smartphones) are connected via the Internet using encrypted and cryptographically authenticated connections (e.g. encrypted VPN with authentication using strong passwords and cryptographic client certificates)
 - Logging of the deletion/destruction of data carriers
 - Use of document shredders (min. security level DIN 66399: P4 with max. 160 mm² per particle and 6 mm strip width or P5 with max. 30 mm² per particle and 2 mm strip width)
-

Organisational measures

- Implemented deletion on development, test and production environments
 - Secure storage of mobile data carriers
-

Encryption acc. to Art. 32 para. 1 (a) GDPR

- Use of strong encryption for mobile devices (smartphones and tablets) and mobile data carriers (e.g. USB sticks, hard drives)
 - All encryption technologies used in production are state of the art
 - Strong encryption of data carriers in laptops & clients
-

1.3. User control

User control describes measures to prevent the use of automated processing systems using data transmission equipment by unauthorised persons. This can also include protection against unauthorised system use and against system intrusion and misuse via networks.

Technical measures

- Use of an anti-virus solution on client computers and notebooks with daily updates of the signature databases

- Use of an endpoint protection system on client computers and notebooks, including automatic on-access scans

- Use of an anti-virus solution or an endpoint protection system on servers

- Use of an anti-virus solution or endpoint protection system on smartphones and tablets

- Checking incoming emails using anti-malware protection

- Wireless access only via current WLAN routers with effective access mechanisms

- Guest WLAN without access to the internal network

- Only software for which security updates are made available in a timely manner is used

- Use of operating systems and software for which security updates are still available

- No mobile devices are used for which there are no (or no longer any) security updates.

- Automatic installation of security-relevant updates and patches for operating systems from client computers

- Proper configuration of software distribution services

- Configuration of automatic security updates for servers

- Prompt manual installation of security updates on risk-prone servers

- Regulated process for installing security updates for browsers and basic components (e.g. Java, PDF reader, remote maintenance software and important company software).

- Use and proper configuration of a hardware and software firewall

- A security concept for the use of printers, copiers and multifunctional devices is in place (e.g. print-to-me, follow-me print, with PIN)

- Logging at network and firewall level to detect and analyse unauthorised access between networks

- Internal network areas with different security levels are separated by firewalls

1.4. Access control

Access control describes measures to ensure the exclusive use of automated processing systems by authorised persons under the scope of their access authorisation and thus guarantees that authorised persons only have access to data covered by their authorisation.

Technical measures

- Login with username & password

- Use of biometric features for login on IT devices or in security zones (e.g. fingerprint, FaceID, etc.)

- For smartphones: access only after authentication (e.g. PIN, password)

- Use of two-factor or multi-factor authentication for admin accounts

- Only strong passwords are used for the admin accounts of the IT systems (e.g. at least 16 characters, complex and without common word components).

- Non-privileged standard accounts also for administrators for other work outside administrative activities.

- No dependency of the entire operation on individual employees with administrator IDs.

- Secure storage of central administration access data (e.g. in a safe) and access options in an emergency.

- Mandatory use of strong passwords according to current recommendations (e.g. by BSI, NIST, ENISA)

- Password manager in use

- Automatic blocking of access in the event of too many failed attempts (temporarily or completely)

Organisational measures

- Centralized password assignment

- Default authentication information assigned by the manufacturer is changed after installation

- Management of user rights by the IT administrator

- Secure delivery of login information for users (e.g. encrypted e-mail, separate letters for user name and password)

- Measures for recognising the compromise of passwords

- Passwords are blocked after a security incident, even if suspected, and must be reassigned by the user.

- Documented authorisation concept including role profiles for employees to control, regulate and manage access to information.

- No administrator IDs for users who do not perform administrative activities.

- Regularly check whether the assignment of roles corresponds to the specifications and whether the roles still meet the requirements of the business activity.

-
- Number of IT administrators reduced to a minimum
-

1.5. Separability

Separability describes measures that ensure that personal data collected for different purposes can be processed separately.

Technical measures

- Implementation of client separation through separation at system level
- Implementation of client separation through separation at data level
-

Organisational measures

- Authorization concept
- Logical client separation (on the software side)
- Separation of access using database rights
-

1.6 Pseudonymisation acc. to Art. 32 para. 1 (a) GDPR

Pseudonymization describes measures so that the data can no longer be assigned to a specific data subject without the use of additional information, provided that this additional information is separately kept and is subject to corresponding technical and organizational measures.

Applying pseudonymization to personal data can reduce the risks to the data of the data subjects. Pseudonymisation is sufficient if de-pseudonymisation by internal users is not possible or only possible with disproportionate effort.

- Not relevant, as no pseudonymisation takes place or is required

2. Integrity according to Art. 32 para. 1 (b) GDPR

2.1. Transmission and transport control

The transmission control describes measures for checking the addressee of the data transmission. Transport control describes measures to ensure the confidentiality and integrity of data when transporting data carriers.

Technical measures

- Transport encryption is implemented only end-to-end.
- In case of mass e-mailing or newsletters, the disclosure of all recipients is prevented by technical or organizational means.
- For messengers: Use of state-of-the-art transport and content encryption of messages and files
- Use of encrypted and password-protected data containers (e.g. ZIP, RAR file)
- No usage of unencrypted protocols (e.g. FTP, Telnet) when transferring personal data
- Remote maintenance of clients for administrative purposes exclusively via encrypted connections after authentication by the administrator and release by the user

Organisational measures

- Careful selection of transport personnel and vehicles
- Secure transport containers/packaging
- For physical transport: personal handover with protocol

2.2. Input control

Input control describes measures for (retrospective) verification of which personal data has been entered or modified in automated processing systems, at what time and by whom.

Technical measures

- Traceability of data entry, modification and deletion through personalised (unique) identifiers in IT applications
 - Logging of access to the server and operating system to detect and analyse unauthorised access
 - Logging access to IT applications with critical data in order to detect and analyse unauthorised access
 - Regular evaluation of log files without cause to recognise unusual entries - preferred: automatic heuristics
-

2.3 Reliability & data integrity

Reliability describes measures that ensure that all system functions are available and that any malfunctions that occur are reported. Data integrity ensures that stored personal data cannot be damaged by system malfunctions.

Technical measures

- Use of signature procedures (qualified electronic signature) for the digitalisation of documents

- Regularly updated firewall and network components

- Regular updates of the spam filter

- Regular updates of the the virus scanner

- Regularly check that the firewall is configured correctly (e.g. by scanning ports for your own IP addresses)

- Hardening measures are implemented (e.g. restriction/deactivation of unnecessary authorisations, ports, protocols, servers)

- Implementation of malfunction alarms for IT systems, applications and when installing new software

- Encryption of the databases of IT applications with critical data

3. Availability and resilience of the systems (resilience) according to Art. 32 para. 1 (b) GDPR

3.1 Recoverability acc. to Art. 32 para. 1 (c) GDPR

Recoverability describes measures that ensure that deployed systems can be restored in the event of a fault.

-
- Documented data backup concept

 - Documented backup policy for servers and end devices

 - Appropriate protection of backups against encryption by ransomware

 - Documented restart concept (measures for immediate restoration of availability in the event of system failure)

 - Checking the data backup process

 - Regular data recovery tests and logging of the process (recommendation: quarterly)

 - Fast restoration of the disaster backup

 - Suitable physical storage of backup media in a secure location outside the server room (e.g. safe, fire protection, physical separation)

 - Storing the data backup in a secure location outside the company (e.g. external encrypted hard drive or second server)

3.2 Availability control

Availability control describes measures that ensure that personal data is protected against accidental destruction or loss.

Technical measures

- Server rooms and/or data centres have smoke detection systems
 - Server rooms and/or data centres have fire alarm systems
 - Server rooms and/or data centres have fire extinguishers or fire extinguishing systems
 - Server rooms and/or data centres have sufficient air conditioning
 - Server rooms and/or data centres have systems for monitoring temperature and humidity
 - Regular checks of the system status of the relevant servers (monitoring)
 - Use of systems to ensure the power supply to server systems (UPS), especially in the event of short-term power failures or fluctuations
 - Server rooms and/or data centres have protective socket strips
 - RAID system / hard drive mirroring
 - Data protection-compliant video surveillance of the server room
 - Logging access to the server room
 - There are no fire protection risks
 - Physical protection of the server room against break-ins
 - No risks from flooding/heavy rain, especially for server rooms in the basement
 - Physical protection of the router
-

Organisational measures

- Complete and up-to-date network documentation
 - Up-to-date device management and documentation is available.
-

4. Procedures for regular review, assessment and evaluation according to Art. 32 para. 1 (d) GDPR

Organisations must not only implement appropriate security measures, but also ensure that these measures are reviewed and evaluated at regular intervals. This process should ensure that the measures taken continue to be effective and meet current requirements in order to minimise data protection risks.

Organisational measures

- Appointment of a data protection officer and communication to staff.
 - Conclusion of data processing agreements with subcontractors in accordance with Art. 28 GDPR
 - Review of technical and organisational measures in accordance with Art. 32 GDPR
 - Centralised documentation of all procedural instructions and regulations on data protection with access for employees as required
 - Documented process for recognising, reporting, handling and following up on security and data protection incidents.
 - Documentation of security and data protection incidents (e.g. ticket system)
 - Regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing
 - List of processing activities within the meaning of Art. 30 (1) and (2) GDPR
-

5. Security of the development environment

5.1 Software development

Data protection and security must be taken into account at an early stage in the development of in-house software systems or when selecting software products for your own company.

Technical measures

- Separation of productive from the development/test systems
 - System and security tests, such as code scans and penetration tests, are carried out
 - Access to source code in software development is restricted
 - Ongoing inventory of the versions of software or components (e.g. frameworks, libraries) and their dependencies
 - Standard software and corresponding updates are only obtained from trustworthy sources
 - Time delays between multiple login attempts (especially when logging in via the Internet)
-

Organisational measures

- Documentation of own IT applications (system description, authorisation concept, interfaces, reports, deletion concept)
 - No storage of personal data or access data in the source code management
 - Data entries are validated according to semantic criteria (semantic input validation)
 - Purpose attributes have been defined and implemented for data fields and records
 - Only synthetic data, i.e. no real data or personal data, is processed in the test and development environment.
 - Display of the number of failed logins for the user who successfully logs in (goal: create transparency for attacks/attempts that have taken place)
 - Relevant employees are trained that security by design (ensuring confidentiality, availability and integrity) as a subset of data protection by design is a legal data protection requirement and has an influence on central design decisions (product selection, centralised vs. decentralised, pseudonymisation, encryption, country of a service provider)
 - Sufficient test cycles are taken into account
 - Ensure that an ongoing plan is in place to monitor, evaluate and apply updates or configuration changes for the life of a software application
-

5.2 Development of web applications (e.g. online shop, apps, etc.)

Websites and web applications are usually easily accessible platforms for attacks, which can usually be well secured using known best-practice approaches.

Not relevant, as no web application development takes place

6. Ensuring processing in accordance with instructions pursuant to Art. 32 para. 4 GDPR

These measures protect data security against internal compromise and reduce the risk of circumvention of the technical security measures by the natural persons entrusted with data processing.

Organisational measures

Confidentiality obligation for contractors

Confidentiality agreements for employees
