Documentation of Technical and Organisational Measures (TOM) pursuant to Article 32 GDPR

dab: Daten- Analysen & Beratung GmbH
dab: data driven services GmbH
(dab:Group)

Hans-Obser-Straße 12
94469 Deggendorf

Technical and Organisational Measures (TOM) pursuant to Article 32 GDPR

of

dab:Group,
Hans-Obser-Straße 12,
94469 Deggendorf

as per 12/2023

Note:
Technical and organisational measures (TOM) are the measures prescribed pursuant to Article 32 of the General Data Protection Regulation (GDPR) in order to ensure security of processing for personal data. According to Article 32 GDPR, controllers and processors are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The measures are to be determined taking into account the state of the art, the costs of implementation and the nature, scope and purposes of processing.

According to Article 24 paragraph 1 and Article 32 paragraph 1, an additional obligation exists to undertake a regular review and update the document where necessary.

1. Confidentiality

1.1 Physical access control

Physical access by unauthorised persons to data processing systems on which personal data are processed or used is prevented through various technical and organisational measures.

State-of-the-art, personalised RFID transponders furnished with individual physical access authorisations are used at the entrances. During this process, issued physical access authorisations are checked to ensure they are necessary and adjusted where required.

Changes that occur between the review cycles are dealt with and implemented immediately.

The documented authorisation concept for using the transponders is checked regularly to ensure it is up-to-date.

Automatically closing doors ensure that physical access to the company is restricted at all times and is only possible for authorised persons via transponders.

Offices and rooms in which confidential data are processed (including those of senior management, amongst others) are always locked when not occupied, even during business hours.

Visitors to the company are welcomed by administrative staff and recorded as part of an internal visitor process. Visitors are always logged in accordance with data protection provisions.

Physical access to the server room is also protected through adequate technical and organisational measures. Physical access is only possible for authorised, technical personnel with a personalised key. In addition, it is ensured that the company's own IT hardware in the server room is always kept secure in locked cupboards.

Locked doors ensure that the main entrances to the business premises are always secured during opening times.

1.2 System access control

Within the company, it is ensured that only authorised staff or senior staff receive access to applications and systems in which personal data are processed. From a technical perspective, an individual ID comprising user name and password is ensured for every member of staff. Passwords have state-of-the-art complexity (at least 10 characters, upper-case, lower-case and special characters). Technical measures ensure compliance with the level of complexity. Employees are also made aware that they must use a different password for each portal. In addition, computers must be locked by activating the password-protected screensaver each time staff members temporarily leave their workstations. Relevant organisational policies exist within the company. From a technical perspective, computers lock automatically after a reasonable period of time.

Within the company, data carriers in notebooks are secured against external system access by means of pre-boot encryption at hardware level.

As a further organisational measure, the company operates a process that ensures that possible losses of mobile devices are immediately reported to the IT departement and dealt with. If a device is lost, the appointed Data Protection Officer is always included in the procedure in order to deal with the matter further and report the incident.

An antivirus software protects client systems against viruses, Trojans and other attacks. The necessary signature updates for the virus scanners are performed at appropriate time intervals. Central patch management is also carried out to ensure that client systems are always provided with the latest security updates.

The company network is protected against attacks by the use of up-to-date firewalls and malware scanners, intrusion detection and intrusion prevention.

Access to IT systems from outside is only possible in a controlled manner either via additional multi-factor authentication or via an encrypted VPN connection. Multi-factor authentication is also required for access via VPN.

In addition to the technical measures, access control is strengthened through organisational rules.

These include internal company data protection and information security policies such as the secure use of mobile data carriers and compliance with data protection and security provisions when working at mobile workstations. Staff members are obligated to comply with all existing policies, thus ensuring that established technical and organisational measures are also used by employees at mobile workplaces. In addition, all staff members are placed under a written confidentiality obligation.

1.3 Data access control

The company adopts state-of-the-art data access control measures for its data processing systems and IT systems. The implemented measures aim to provide adequate protection from unauthorised reading, modification or deletion of data by unauthorised persons. Here, the company uses data protection containers to dispose of information and documents that are no longer required. The contents of these containers are collected at regular intervals by a certified service provider and disposed of pursuant to DIN 66399, in accordance with data protection requirements. This ensures that even after disposal, personal data are protected against unauthorised access.

Prior to decommissioning, all data carriers are generally erased using an appropriate procedure; where necessary, they are also mechanically destroyed in compliance with the GDPR.

From an organisational perspective, a documented rights and roles concept exists for all IT systems and applications. This includes in-house concepts for filing documents on the file server infrastructure and for the CRM system used. Individual

authorisation management enables differentiated control of access to personal data. The issued authorisations are regularly reviewed and adjusted as needed. In particular, authorisations are changed immediately where a new staff member joins the company, in the event of an internal change, or if an employee leaves the company. Authorisations are only issued, amended or withdrawn following explicit approval by senior management or appropriately authorised persons. Data access authorisations are only managed by administrators. Administrator accounts are restricted to a minimum and are only available to a select group of individuals. Access to personal data is regulated in such a way that employees only receive access to data that they require in order to fulfil their respective roles. The company bases this on the "need-to-know" principle.

1.4 Segregation control

The company uses segregation control measures to ensure that data are always processed according to the respective purpose. Appropriate techniques ensure that personal data of customers, clients and the company's own data are processed physically or logically separated from each other. Where necessary, care is taken to ensure client capability for relevant applications. Productive and test systems are segregated from each other. From an

organisational perspective, segregation control is achieved through authorisation concepts and the specification of database rights. Personal data are managed in different Windows project folders, which are also encrypted. This enables strict segregation during processing.

2. Integrity

2.1 Data transmission control

Data transmission control measures ensure that data are protected against unauthorised modification, and also from unauthorised reading or copying. To be able to ensure this, only encrypted connections based on VPN or SSL technologies are used for data transmission. Care is taken to ensure transmission encryption when using emails. Where confidential data are transmitted via email, additional content encryption based on password-protected attachments is used. The associated password is transmitted to the recipient via a separate channel such as the telephone. In the case of general transmission of personal data to external recipients, the duration for which the data are provided and any necessary deletion dates are checked and complied with. To comply with this measure, the company has a separate deletion concept which takes GDPR requirements into account. The Information security management systems control measures are described in detail in the company's information security management concept.

Where necessary, confidential data transmitted on external data carriers are secured through adequate cryptographic processes. Where possible, personal data are pseudonymised or anonymised.

Special precautionary measures are applied for external data that are provided to the company by customers within the context of data analytics projects. Here, it is ensured that data are only stored on encrypted data carriers and that processing is always regulated through explicit agreements and declarations of consent with the customer.

2.2 Input control

Input control measures aim to make it possible to guarantee traceability where data are input, modified or deleted. Within the company, this is ensured through organisational measures under which individual user names are used in place of user groups. Only authorised employees are able to make changes to personal data, depending on their role and activities.

In terms of software, changes to personal data are recorded by logging master data and transaction data, including a change history. The logs can only be viewed by authorised people. This ensures precise traceability within the systems, thereby ensuring GDPR-compliant input control.

3. Availability and resilience

3.1 Availability control

The company implements state-of-the-art measures to ensure the continuous availability and resilience of personal data and information. The implemented measures aim to guarantee permanent protection against data loss, incidents or other damaging events.

To achieve this goal, IT systems in two server rooms are each connected to two uninterruptible power supplies (UPS). The servers are secured against each other in a high-availability cluster.

In addition, both server rooms are equipped with a redundant air conditioning system, which is equipped with temperature controls and a humidity control system. A fire alarm system is installed to protect against fire.

To ensure correct implementation of the physical measures can be checked, the server room undergoes regular audits by the Data Protection Officer.

From an organisational perspective, a tried-and-tested backup & recovery concept exists which can be used to restore business-critical IT systems and data in the shortest possible time. Backup procedures are checked and logged. Data recovery tests are also conducted at regular

intervals. System redundancy exists at all times for the primary IT systems. The backup strategy is designed so that backups are carried out at regular and documented intervals, depending on the criticality of the respective system.

The systems are additionally integrated into a comprehensive system and network monitoring process to ensure a prompt response to malfunctionings in the event of a fault. Penetration tests are conducted where necessary to check the resilience of the IT infrastructure. Malfunctionings of the Internet connection can be offset by a corresponding backup line.

3.2 Data protection management

To meet the requirements of the General Data Protection Regulation, adequate organisational data protection management processes have been established within the organisation. These aim to ensure continuous implementation of data protection within the company. The company uses data protection management software to manage the established processes, tasks and documentation.

The company has appointed an external Data Protection Officer. He advises and informs the controllers, the individuals affected or the processors in data protection matters. He monitors compliance with the requirements of the GDPR and the internal data protection agreements, and works with the competent supervisory body. Where required, data protection impact assessments are carried out for necessary processes or technologies. In such cases, the Data Protection Officer contributes his specialist knowledge. The company complies with the obligations to provide information pursuant to Article 13 and Article 14 of the GDPR. All employees enter into a written confidentiality agreement and are made aware of its importance. Implemented policies and technical measures are designed so that they can also be complied with by employees working at mobile workstations. When they join the company, employees undergo initial data protection training to make them aware of their obligations. The Data Protection Officer is also included in further, regular measures relating to employee awareness. The internally appointed Information Security Officer additionally develops measures and guidelines to ensure that planned IT security strategies can be effectively implemented.

This is based on the international standard for information security ISO/IEC 27001. The established information security management system has been rolled out and is known to all employees.

3.3 Order control

If third parties are commissioned to process personal data, suitable measures ensure that data are only processed in accordance with the client's instructions. All contractors are selected based on diligence considerations with regard to data protection and data security. Necessary contracted data processing agreements are always concluded with all contractors. Existing contracts undergo regular checks by the Data Protection Officer to ensure their contents are correct. Other subcontractors are not generally used. If personal data are transmitted to a third country, the requirements of Articles 44 et seqq. of the GDPR are complied with. If this is necessary, the relevant requirements of data protection law are also checked, and approval is exclusively given by the Data Protection Officer as a recommendation for senior management. Confidentiality agreements and data processing agreements are always concluded with service providers who work for the company on an extended basis (e.g. website implementation).

In accordance with Article 25 GDPR, the CRM system used guarantees the necessary privacy-by-default settings, taking into account the costs of implementation and the state of the art. Specifically, this means safeguarding the principles for the processing of personal data in accordance with Article 5 of the GDPR, such as, for example, restrictions on storage and data minimisation. Such compliance can prevent a data-protection incident.

4. Updating of measures

The technical and organisational measures are reviewed at least once a year to check that they are up-to-date and appropriate, and are adapted where necessary. The outcome is documented in each case. If significant changes to the implemented measures arise outside of the review cycle, the documentation detailing the technical and organisational measures is directly adapted. Each review of the implemented measures checks that data protection measures are designed in such a way (using technology engineering and privacy-by-default settings) as to ensure that the state of the art is always taken into account.

5. Change history

Version	Author	Change	Date
1.0	Thomas Greiner	Erstellung	05.10.2020
1.1	Tobias Damasko	Änderung / Überprüfung	15.02.2022
1.1	Stefan Wenig	Freigabe	16.02.2022
2.1	Michael Paternoster	Änderung / Überprüfung	29.11.2023
2.1	Stefan Wenig	Freigabe	27.02.2024