Standard Data Protection Measures (Standard TOMs)

Measures for achieving the data protection goals pursuant to Articles 5 and 32 GDPR

Contents

Introduction

Content

This document describes the standard data protection measures of Schwarz Group for ensuring compliance with the data processing principles set out in Article 5(1) of the EU General Data Protection Regulation (GDPR), including the technical and organizational measures (TOMs) pursuant to Article 32 GDPR. Any project- or system-specific deviations from these measures or supplemental measures must be documented separately in the respective processing form, the "TOMs for applications and IT systems" checklist or, where applicable, the data processing agreement.

Section 1: Measures for ensuring compliance with data processing principles

Legal basis: *Article 5(1) GDPR*

The following measures are designed to ensure compliance with the principles relating to processing of personal data pursuant to Article 5(1) GDPR (data processing principles).

1. Lawfulness, fairness and transparency

Legal basis: *Article 5(1)(a) GDPR*

The department responsible for the process (the controller) documents in the record of processing activities all processes, IT systems and other processes in which personal data are processed. The processing form prepared for the relevant process includes any and all information related to data protection, in particular the purposes for which the personal data were processed as well as the scope, source and time limits for erasure of such personal data. Additionally, the form must also include information about the intended analyses, the nature and scope of the data subject's information, the data flow and the IT systems used, and the transfer to internal or external bodies, both within and outside the EU/EEA.

When processes, IT systems or other procedures are redesigned or modified, the Data Protection department must be involved as early as the conceptual phase. Every documented process is assessed for lawfulness, fairness and transparency on the basis of the information in the processing form, in order to ensure compliance with such principles and the duties to provide information to data subjects in order to enable them to understand the nature and manner of the data processing. The responsible person within the department decides whether or not to approve the implementation of the process based on this assessment. This process is repeated any time processes, IT systems or other procedures are changed.

2. Purpose Limitation

Legal basis: *Article 5(1)(b) GDPR*

The purposes for processing personal data are defined in advance and documented in writing in the record of processing activities in the relevant processing form. Suitable technical and organizational measures are implemented to ensure that personal data are not processed further in a manner that is incompatible with the specified purposes (see Section 2 below).

3. Data Minimization

Legal basis: *Article 5(1)(c) GDPR*

When new processes, IT systems or other procedures are introduced in which personal data are processed, any consultation on the relevant data protection implications must take into account the requirements of privacy by design and privacy by default in order to work toward ensuring compliance with principle of data minimization. This must already be done in the design phase by ensuring that only such data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed Where feasible and cost-effective, personal data must be pseudonymized in the systems. Furthermore, for systems with their own user interfaces, measures must be implemented to enable the data subjects to decide the scope of the data processing themselves, or at least to influence this.

4. Accuracy

Legal basis: *Article 5(1)(d) GDPR*

When new or existing processes, IT systems or other procedures in which personal data are subject to automated processing are designed or modified, suitable measures for establishing the integrity of the data (see section 2 no. 2) must ensure that the data are accurate and, where necessary, kept up to date. Erasure and rectification measures must ensure that inaccurate data are erased or rectified without undue delay.

Furthermore, the responsible departments must ensure that the personal data entrusted to them are accurate.

5. Storage limitation (erasure)

Legal basis: *Article 5(1)(e) GDPR*

Standard time limits for erasure must be stipulated in the processing form of the record of processing activities when documenting the processes, IT systems and other procedures to ensure that personal data are stored for no longer than is necessary for the purposes for which they are processed. Once the standard time limits for erasure expire, the data must be erased or fully anonymized by removing any personal data. Depending on the procedure stipulated in the processing form, this must be done automatically or manually. For verification purposes, standard control mechanisms must be implemented for systems where data are erased manually.

6. Accountability

Legal basis: *Article 5(2) GDPR*

The duties of accountability specific to data processing under Article 5(2) GDPR must be complied with by documenting and regularly updating the relevant information in the record of processing activities and by stipulating the requirements for data processing-specific documentation duties such as consent.

Section 2: Technical and organizational measures (TOMs)

Legal basis: *Article 32 GDPR*

The following measures serve to ensure compliance with the requirements relating to the security of processing personal data by implementing appropriate technical and organizational measures pursuant to Article 32 GDPR.

1. Confidentiality

Legal basis: *Article 5(1)(f) in conjunction with Article 32(1)(b) GDPR*

The following measures must be taken to ensure the confidentiality of data on a permanent basis.

1.1 System access control

The following measures must prevent unauthorized persons from gaining physical access to data processing facilities.

1.1.1 Anti-burglary measures, fire and lightening protection

As a rule, buildings are fenced in and access roads are gated. If this is not the case in individual instances, the following and, where necessary, additional measures must ensure appropriate access control. External doors must be secured with security locks. Lightning protection systems must ensure that energy spikes and surges are conducted away from buildings. Data centers must be equipped with burglar alarms. The control center must be notified in the event a data center door is forced open. Facilities must be equipped with fire detection devices. Fire alarms, the deployment of extinguishers, water ingress and power outages must be monitored centrally by the control center. Other alarms must be forwarded to site security or the emergency call center who must then notify the appropriate individuals/authorities pursuant to the alarm notification list.

The data center must be equipped with a gaseous fire suppression system. Portable CO2 fire extinguishers must be located in sufficient quantity near the doors of the data center and the server rooms.

1.1.2 Key management

Office buildings are locked at all times. Doors may only be opened by authorized personnel using an electronic key card or a mechanical key. Office keys and locks must be assigned on the basis of a hierarchical access control system, meaning that direct supervisors can access the offices of their employees. Offices in which personal data are processed are locked when employees leave for extended periods or after office hours. Confidential data in open-plan offices is locked away in office furniture.

Master keys for central locations are locked away and secured with alarm systems with site security or in the control center. In the event of fire, master keys are provided to the fire brigade to allow it access without the use of force. The issue and return of keys is recorded.

1.1.3 Electronic access protection

When presented, electronic employee ID cards unlock and lock entry doors to buildings, doors to building floors and hallways as well as access doors to secured areas. The electronic access profiles are generally based on the employee's

department and position. There are also functional profiles for janitorial and maintenance staff, for example.

The issue, respective access permissions and use of electronic ID cards are logged. Access to these data must be granted by the responsible facilities management employee, site security and the respective system administrator in accordance with the documented authorization concept.

1.1.4 Access for guests

Central locations have reception areas where visitors can sign in during business hours. An employee receives the guests in the waiting area and escorts them during their stay on the premises. The doors must be locked outside of reception hours or when the reception areas are unstaffed. In such instances, visitors must contact the employee via the telephone in the reception area or site security when visiting central locations.

Handymen and cleaning and maintenance personnel must be given electronic ID cards with additional access rights; their access to secured areas must be restricted, however. They must be given instructions for their activities in the buildings and supervised by employees of the responsible department; site security will escort them at the department's request.

1.1.5 Data centers

The location, buildings, rooms, etc. must be subject to clearly defined structural specifications pursuant to the current building specifications and security concepts for data centers. Central IT components must be housed exclusively in lockable rooms. The same must apply to the central components of the telecommunications system. The power supply must be secured via a separate electrical sub-distribution unit with a UPS and an emergency generator. The UPS must be capable of supplying emergency power for a set minimum amount of time. Meters must be used. Functionality tests must be conducted regularly.

Service technicians (power, water, extinguishing systems) not in possession of their own access card must be provided with a visitor's card when signing in and escorted by site security or an employee of the data center's operator with a valid ID card. IT equipment service technicians must be escorted by the specialist team or by site security.

1.1.6 Video surveillance

Video cameras must be in place to monitor access to sensitive areas of the area. Video footage generally must be stored for 7 days.

1.1.7 Network

The local area network (LAN) must consist of different functional and security zones. Firewall rules or access lists must regulate access between the zones.

Active network components outside of the data center must be housed in locked utility rooms. If this is not possible, they must be installed in lockable cabinets. This excludes access points mounted to ceilings for the purposes of illuminating the facilities.

Depending on the location, access controls to the network must be conducted via secure protocols (e.g., 802.Ix). When accessing the network, users/end devices must be identified prior to receiving the IP address.

WLAN connections must be encrypted and WLAN users must be authenticated, including on the basis of certificates. Certificates and WLAN access must be managed centrally. Users of the guest WLAN must receive access to an Internet connection only.

1.2 User, access, data media and storage control

The following measures must ensure that unauthorized persons cannot read, copy, change or erase personal data on data media and in data processing systems and that those persons authorized to use a data processing system have access only to the data they are authorized to access.

1.2.1 Authorization concepts

Authorization concepts must be included in the system documentation. Authorizations must be granted on a need-to-know basis. Compliance with the respective authorization concepts must be regularly reviewed. Unused user accounts must be deleted.

Authorization concepts – from centralized user management to server and folder authorizations in combination with network segmentation access controls – must grant users access across systems and applications to the IT resources they need to complete their work depending on their roles and duties within the company.

1.2.2 Passwords and PINs

All access to IT systems must be regulated via passwords and user accounts. User accounts must generally be clearly assigned to one person. A personal password must be assigned when a user registers for the first time. The password procedures stipulated by the system must meet the various functional requirements of the user accounts, including the strict security requirements for data and systems. Passwords must be changed regularly depending on the security requirements and the risk situation.

Small, mobile devices such as smartphones and tablets must be permanently assigned to the respective user. For economic and ergonomic reasons, an exception to the password guidelines must apply to the length of PINs for such devices. Depending on their features and configuration, mobile devices must be identified using centrally-managed device certificates in order to automatically establish a connection with the network when in range of a company WLAN.

1.2.3 Anti-theft protection for laptops

The hard drives of laptops must be encrypted, thus requiring a personal password to be entered upon starting up the laptop.

1.2.4 Administration of IT systems

As a rule, the contractor must deploy its own employees for managing the supported IT systems. Pursuant to their employee agreements, IT employees must be bound by telecommunications and data secrecy.

Administration access must be used exclusively for administrative purposes and subject to extensive record-keeping measures. Logs must be stored such that they are protected from being altered and must be regularly analyzed on a test basis.

Role concepts must ensure that the administrative rights needed for the tasks and duties have been documented and verifiably granted. Administration accounts must be personalized. Administration accounts must be distinguished from normal user accounts using an identification marker in the user name.

Administrative authorizations on systems containing personal data must be approved using the principle of dual control and be subject to regular reviews.

Network infrastructure components must be administered by authorized management systems via controlled connections. Network administrators must be identified via central authentication mechanisms.

1.2.5 Strong authentication

Access by external users from public networks must be identified using two-factor authentication. The two factors must be a one-time password and the user's personal password. One-time passwords may be valid for a limited time only and displayed on the physical token generator, software token, etc. upon entering the PIN. Token generators must be issued by the Service Desk. Receipt must be confirmed in writing and the user must be informed that in the event the token generator is lost, the Service Desk must be notified immediately so that the generator can be blocked. The generator must be automatically locked after a certain number of failed log-in attempts. Independent departments must be responsible for approving remote access requests and operating the administrative systems for token generators.

Site-2-site VPN tunnels must be installed for enabling communication to and from external IT systems with contracting parties. The public IP addresses of the firewalls on both sides, clearly defined encryption parameters and a password agreed by telephone ensure secure authentication and encryption.

1.2.6 Remote access

Remote access by administrators must be subject to multilevel security protocols. Administrators must work in one or more virtual environments. Activity must be logged and reviewed when justified.

1.2.7 Remote servicing via Service Desk

Logged-in users must accept a remote access request to grant Service Desk employees control over an IT workplace. Remote servicing sessions are visible on the monitor and the user may intervene using the mouse or keyboard at any time. Connecting remotely is not possible if the computer is shut down or the workstation has been locked. If during a remote session a Service Desk employee notices that documents or applications containing confidential information are open, the Service Desk employee must ask the employee to close the documents or applications before continuing.

1.2.8 Client security measures

BIOS passwords and interface control software must ensure that users use supported hardware for its intended purpose only. The transfer of data to removable media such as USB sticks must be regulated. Removable media must be granted access on a case-by-case basis upon request and must be automatically encrypted prior to being used for the first time. The Information Security Officer's special permission is required to enable unencrypted removable media.

Client network communication must be kept to a minimum using centrally-managed system settings and hardware control tools. Laptops must also have local, centrally-managed firewalls. When outside of the company network, laptops may briefly use third-party networks to establish a VPN tunnel with the company network. Once a connection is established, the concurrent use of other network connections such as via hotspots is prohibited.

Software must be installed centrally. Users may request software from company's software catalog. Once permission is granted by the supervisor, the application may be installed. Decisions to install software not included in the catalog are made on a case-by-case basis.

PC workstations must lock automatically after a certain period of inactivity, preventing documents from being inspected or programs from being launched. PC workstations must be unlocked by entering the logged-in user's password or by signing in as an administrator.

1.2.9 Requesting authorization

Employees, supervisors and administrative assistants may submit authorization requests. The requests must be implemented centrally once approved by the supervisor. Furthermore, access to particularly sensitive resources requires the approval of the respective data owner. The deletion of authorizations must be requested, justified and documented. Operational processes are set out in the Identity Management (IDM) manual. Data and systems owners must receive periodic reports about users and authorizations. SAP authorizations must be automatically reviewed using a special software solution. Problematic combinations of rights and unused accounts must be deleted.

1.3 Transfer control

The following measures ensure that no personal data can be read, copied, modified or removed without authorization when it is electronically transmitted, or during its transport or storage on data media, and that the intended point of transmission by data transmission equipment can be checked and identified.

1.3.1 Logs

Log settings generally depend on the system specifications, the operating requirements and the security requirements. Where high levels of security are stipulated, log data must be archived in line with the system-specific storage periods and protected against manipulation.

1.3.2 Functional zones

Functional zones must be in place. Firewalls must regulate access and data flows from and to these zones.

1.3.3 Printing

Printers, copiers and multifunction devices must be outfitted with devices capable of scanning/reading electronic ID cards. Confidential print jobs may not be executed until the user has been authenticated.

1.3.4 Internal exchange of data

Network drives and database-driven applications must be made available to authenticated and authorized employees for exchanging data. Access authorizations must be implemented using authorization concepts and central user management systems, and logged by the relevant systems. Network and system environments must be documented.

1.3.5 Interface control using disk encryption

The use of hardware, particularly removable media and devices that are connected to PCs or laptops via USB or similar ports, must be monitored in order to prevent the unauthorized transmission and uncontrolled outflow of electronic information.

With respect to write permissions, removable storage media such as USB sticks may only be used upon request and with supervisor approval.

The data on the removable media must be password protected.

The data media of iOS devices must use AES-256 encryption. Android users must activate encryption.

If needed, individual files may be encrypted with a password-protected AES-256 key using a file compression program available at all workplaces.

1.3.6 Procedures in event of a loss of hardware

Employees must be informed about the procedures to be implemented in the event hardware becomes damaged or lost. Appropriate data protection measures must be implemented in the event of loss or damage. These include resetting the hardware to factory settings to render locally-saved user data unusable, or blocking the account associated with the device from using the company's central services.

1.3.7 Transport (mail)

The transport/dispatch of data media is subject to strict limitations and only permitted for the exchange of data with partners and service providers. Registered mail or similar additional services must be used when dispatching personal data on removable media via external postal service providers. The Mail Services department must take delivery of, sign for and internally forward any incoming mail.

1.3.8 Use of Internet and e-mail

Users must use predefined web browsers (e.g., Internet Explorer, Firefox) to access websites. In the event of critical vulnerabilities, the browser in question must be blocked by headquarters until the vulnerability is remedied; a corresponding information page must be displayed informing users of the security measure.

Company e-mail accounts may not be used for private purposes.

E-mail users must be given a new, personalized ID when their e-mail account is created. E-mails within in the group must be internally sent and received. E-mails to external recipients may be encrypted using "Secure/Multipurpose Internet Mail Extension" (S/MIME) and TLS. S/MIME must be requested and installed centrally.

1.4 Destruction of data media

Unused data media such as hard drives and backup tape drives must be destroyed by appropriate means, including, for example, using certified professional data destruction service providers. The data media must be formatted and overwritten multiple times. Physically defective data media must be made unreadable through degaussing.

2. Integrity

Legal basis: *Article 5(1)(f) in conjunction with Article 32(1)(b) GDPR*

The following measures must be implemented to ensure the integrity of data on a permanent basis.

2.1 Input control

The following measures ensure that it can be reviewed and determined whether personal data was entered into, changed or removed from a data processing system, and by whom and at what time such activity occurred.

2.1.1 Authorizations concepts, logging and log evaluation systems

As is described in detail in the "User and access controls" section, the central user management system must ensure that IT systems are used in line with the respective roles and authorization concepts. Employees must be assigned read, write or delete permissions depending on their duties and positions. Particularly sensitive data must be encrypted before they are stored in the database to ensure that they cannot be viewed by the database administrators.

Log files must record whenever personal data are accessed. System administrators may view but not change log data. Log data must be manually analyzed in the event of irregularities or security breaches. For particularly sensitive data, logs must be regularly checked for irregularities on a sample basis, including with the assistance of log and log analysis systems.

Changes to user rights must be recorded irrespective of the rights management system and corrected in the case of an error.

2.2 Data integrity

The following measures ensure that any stored personal data are not damaged due to a system malfunction.

2.2.1 Databases

Network segmentation and firewall rules must generally prevent clients and users from directly accessing databases. Access to databases by applications must be authenticated through password-protected database user accounts. Passwords must be changed regularly irrespective of the security requirements for the data.

2.2.2 Functional zones

Production, development and test systems must generally be kept separate in order to minimize the probability of adverse effects due to software or user error and to ensure the effectiveness of the implemented technical and organizational measures.

2.2.3 Protection against malware and measures in the event of security incidents

Signature-based detection methods must be used to protect against malware. Heuristic- and behavior-based methods must also be used. The signatures of the end devices must be automatically updated on a daily basis.

Security administrators must be notified via the central management system in the event of suspicious activity due to malware. Infected data must be quarantined for subsequent analysis and the malware deleted. Should program files be rendered unusable, the clients in question must be re-installed. If the malware cannot be successfully deleted, the infected system must be isolated from the network and scanned with an anti-virus program not requiring a network connection. Following isolation and disinfection, the source of infection must be retraced and countermeasures established to prevent future infections.

Vulnerability scanners must be used. Vulnerability reports for external IP addresses must be regularly sent to the system administrators; non-critical vulnerabilities must be remedied with the help of Patch Management. Depending on the attack vector, critical vulnerabilities must be remedied as quickly as possible using emergency procedures and a permanent record of the progress kept. In addition, the latest information on vulnerabilities and current attacks must be collected from pertinent websites and other channels, e.g., the Federal Office for Information Security's IT Situation Center and private service providers. The relevancy of the information must be reviewed and in critical cases emergency measures must be coordinated centrally. Emergency measures must include rules implemented on the central security systems and Internet, e-mail or other network connections must be partially or fully disabled. Emergency measures must remain in place until the vulnerability is permanently remedied. If there are indications that sensitive systems or data may have been affected or that, for example, malware has infected multiple systems, management must be notified immediately and a team assembled comprising system administrators and IT security experts until the effects are contained and the risk has been eliminated. Critical incidents must be documented immediately and follow-up measures initiated to prevent these or similar incidents from reoccurring.

2.2.4 URL and spam filters

Access to websites must be secured by URL filters with malware protection on Internet proxies. Access to mature, illegal or harmful content must be blocked and filter lists automatically updated. In addition, manually generated filter lists must be used to protect against dangerous Internet connections that the above sources have made public but that have not yet been categorized by proxy developers.

Spam filters, among other measures, must be used to protect against spam and phishing e-mails. The filters must be updated automatically several times daily. E-mail servers must reject obvious spam and phishing e-mails. E-mails with invalid e-mail recipients must be automatically sorted, followed by the validation of the signature, pattern and reputation. If spam or other suspicious e-mails are not properly identified, the recipient must save and send these to the Service Desk or directly to the Spam and Phishing Support e-mail address. Appropriate filter rules must be created if the e-mails are in fact spam or phishing e-mails.

2.2.5 Software control and updates

Windows applications and operating system updates must be managed centrally. Updates must be tested in dedicated test environments as part of the change and patch management process. After successful testing, the update packages must be made centrally available. The updates must not be deployed immediately so that any issues that did not arise during the testing phase can be identified in due time and remedied. The urgency, effects and service times must also be factored into the deployment. An accelerated procedure must be implemented in the case of emergencies. The respective product managers must notify the employees concerned about the established central lines of communication.

Updates for devices whose settings are not managed centrally are the responsibility of the respective users. Users must be informed of their duty to properly maintain the systems when they are issued a device. Updates for mobile devices whose system settings are managed centrally must be tested by Change and Patch Management. After successful testing and in the case of critical updates, users must be notified so that they can install the updates in a timely manner. The version must be centrally monitored and documented.

3. Availability

Legal basis: *Article 5(1)(f) in conjunction with Article 32(1)(b) GDPR*

The following measures must be implemented to ensure the availability of personal data on a permanent basis.

3.1 Availability control

The following measures ensure that personal data is protected against destruction or loss.

3.1.1 Firewall and anti-virus systems

Firewalls and anti-virus systems with multiple levels of redundancy must protect the entire IT infrastructure against Denial of Service (DoS) or similar attacks, malware and unauthorized access via network connections.

3.1.2 Development and test systems

With regard to their key functions, development systems must be equivalent to production systems. When necessary, test systems must be furnished with realistic data. This is to ensure that software updates, expansions and changes are developed and tested for interoperability, compatibility and fulfillment of the requirements without adversely affecting the production environment.

3.1.3 Central file directory

Users must store production data on the central data media on the company's secure network. Data on file servers must be backed up on a daily basis.

3.1.4 Data cabinets

Access to data media safes must be strictly restricted. They must be located in different fire compartments or buildings than the servers, have double-bit key locks, be fire resistant and equipped with separate data media archives in accordance with S 120 DIS. The specifications of the data media safes must be documented.

3.1.5 Climate control for data centers

The data center must be equipped with an electronically controlled air conditioning unit. The temperature must be permanently monitored. The lockable server cabinets must be housed in a cold aisle containment system.

3.1.6 Fire protection measures

The fire alarm systems with automatic notification signals must conform to the established standards. Fire compartments in the data center must be equipped with F90/T90-rated fire doors designed to withstand 90 minutes of fire and smoke. In the event of fire, the gaseous fire suppression system must flood the server rooms with the extinguishing agent. Hallways must be equipped with sufficient numbers of readily identifiable fire extinguishers.

Smoking must be prohibited in buildings. Building stories must be equipped with fire extinguishers. Fire safety regulations for buildings must be available for inspection in the Occupational Safety & Environmental Protection department. Fire drills must be regularly held under the supervision of evacuation assistants. The evacuation system must comply with German BGV A1 principles of prevention.

3.1.7 Power outages or surges

Sensitive systems must be connected to passive and active emergency power supply systems. In the event of a power outage, the battery-operated uninterruptible power supply (UPS) must ensure that the system continues to operate significantly beyond the time the diesel generator begins to generate electricity. The UPS' surge protector must protect the current collector from damage caused by voltage spikes. The operational readiness and proper functioning of the emergency power supply system must be tested at regular intervals.

3.1.8 Emergency management

Given the possibility that IT operations may become restricted, contingency plans must maintain IT-supported business processes. The plans must include the requisite details for the technical and organizational emergency measures.

3.2 Resilience

Redundancies must ensure that material IT services and data remain available in the event of a hardware malfunction. Data center hardware, in particular servers, network components, network adapters, hard drives and fans, must be positioned so that they are easily accessible. Data must be mirrored.

3.3 Restoring data and systems

The following measures must ensure that systems can be restored in the event of a malfunction or disruption.

3.3.1 Restoring and backing up data

In an effort counter system errors, servers must be backed up daily: incremental backups on weekdays and full backups on weekends. The documented backup procedure must be a two-step process so as to minimize the effects of backups. Some of the backup tapes from the data backup devices must be vaulted.

Depending on its criticality, destroyed or lost data must be restored using high availability measures or data backup procedures. The criticality of data restoration depends on the security requirements for ensuring availability. The duration of the tolerable down time determines the maximum time allotted to restore data and thus the procedures selected.

3.3.2 Restoring files

To a certain extent, users may restore accidentally deleted files themselves. In other cases, the Service Desk must be involved.

4. Pseudonymization

Legal basis: *Article 32(1)(a) GDPR*

To the extent possible and appropriate for processing purposes, personal data must be pseudonymized. The corresponding measures must be documented for each process, IT system or other processing.

5. Encryption

Legal basis: *Article 32(1)(a) GDPR*

5.1 Encryption procedures

5.1.1 General guidelines

The effectiveness of the encryption methods and procedures as well as the associated processes for managing the electronic keys and certificates must be reviewed at regular intervals and on an ad hoc basis. In the event new methods and procedures are needed, economically reasonable transition periods must be implemented for phasing out existing systems while concurrently introducing compensatory measures.

5.1.2 Databases

Databases and data sources must be classified pursuant to the security requirements for the data in question. Depending on the requirements in accordance with the level of security needed, Transparent Data Encryption (TDE) must be used for databases. Databases with varying levels of required security must be operated on separate systems. Sensitive data must be made unrecognizable in the event databases are exported to environments with lower levels of security.

Any database access or activities on the part of administrators must be logged and reviewed for irregularities in the event of suspicious activities.

5.2 Transport controls

The following measures ensure the confidentiality and integrity of data during the transfer of personal data as well as the transport of data media.

The transport of highly sensitive data on central systems must be encrypted. Depending on how the data are to be used, connections must be established using HTTPS or VPN tunnels with encryption parameters that are currently considered secure. Data media such as laptop hard drives must be encrypted automatically via software without user input. Certificates used for encryption and signatures must be managed centrally.

6 Testing, assessing and evaluating effectiveness

Legal basis: *Article 32(1)(d) GDPR*

6.1 Reliability

The following measures ensure that all system functionalities are available and any malfunctions are reported.

6.1.1 Processes and procedures

The information security processes and procedures must be defined as part of the information security management system (ISMS) in accordance with ISO/IEC 27001 *et seq*. and reviewed regularly and updated as needed. The ISMS

must include the information security policy, information security principles, standards and processes for comprehensively protecting information and data, and the continuity of IT-supported business processes.

The efficiency and effectiveness of the protective measures must be ensured using the security processes and procedures of the security management system and the reporting. To this end, IT systems must be classified in accordance with the requisite security requirements on the basis of a risk-based analysis. Availability in crisis situations must be ensured through procedures for acute emergencies and security incidents. Preventative measures must be implemented to identify and remedy vulnerabilities before the adverse effects take hold. Employee training and sensitization must be used to bolster employee awareness and support for these measures.

6.1.2 Guidelines and standards

Technical standards and organizational guidelines must be documented and binding. Affected users must be informed of the standards and guidelines as well as how they are to be applied. Any deviations must be requested, approved, and centrally documented.

6.1.3 Security requirements analysis

The procedure for determining the security requirements for data and IT systems must be set out in the security requirements analysis process. The process must be used not only for new systems but also for existing systems with new interfaces; the process must be initiated whenever there are changes to the data flow or content of the data.

The security measures must be based on the security requirements. If existing security measures are insufficient, new measures must be developed, planned, and implemented. If new measures are used on a regular basis, these must be incorporated as the standard or in the guidelines.

Compliance or non-compliance with security measures must be assessed via spot tests, security audits or reviews.

6.1.4 Security reviews/audit framework

New systems must undergo a security review as part of the acceptance review. The systems may be approved only if no critical vulnerabilities are found. Exceptions are only possible through the assumption of risk, but not for public websites.

7. Processing in accordance with instructions

Legal basis: *Article 32(4) GDPR*

The following measures ensure that personal data are processed only in accordance with the instructions of the controller.

7.1.1 Employee sensitization

Employees are bound by data confidentiality and appropriately instructed on the issues of data protection and information security, e.g., through training and measures to raise awareness.

7.2 Control of instructions

The following measures ensure that personal data processed as part of an assignment are processed only in accordance with the instructions of the controller.

7.2.1 Data processing on behalf of the Customer

Where processing is to be carried out on behalf of a controller, the proper contract drafting and engagements must, as a rule, be carried out using model agreements. If a company of Schwarz Group is engaged to process personal data, this must be done on the basis of the respective applicable master agreement on the transfer of personal data within Schwarz Group and using the model agreement for the processing of personal data in individual cases ("Individual Engagement").

Processors must disclose the technical and organizational measures taken prior to processing. Depending on the individual case, it is decided whether additional audit measures will be introduced in addition to the document-based audit of the technical and organizational measures.

7.2.2 Security review of the processor

Prior to commissioning data processing on behalf of a controller, the controller duly verifies that the processor complies with the promised technical and organizational measures. Depending on the responses and the documents provided by the processor, it must be decided whether further measures are required, such as on-site inspections or

the engagement of third parties to verify the level of data protection afforded.

8. Data portability

Legal basis: *Article 20 GDPR*

If data subjects themselves provide personal data, such personal data must, at the request of the data subject, be provided to the data subject or – where technically feasible – on instruction of the data subject to another controller in a structured, commonly used and machine-readable format.

9. Multi-client capability

Legal basis: *Article 5(1) GDPR*

The following measures ensure that personal data collected for various purposes can be processed separately.

9.1 Separation by client

If IT systems process personal data from more than one controller, the data must be processed separately (separation by client). The client separation measures must be documented for the respective process, IT system or other processing.

9.2 Data retention areas

Network segments for retaining data must include only database servers. Mandatory logs of database access are kept.

Databases with varying levels of required security must be operated on separate database servers.

10. Separability

Legal basis: *Article 5(1) GDPR*

The following measures ensure that personal data collected for various purposes can be processed separately.

A three-tier architecture must be used for systems with strict security requirements: There must be one network segment per tier. Firewalls may only allow point-to-point connections between the systems of the presentation tier and the application tier or between the application tier and the data storage tier. Users may access the presentation tier. Only system access is permitted from the presentation tier to the application tier and from the application tier to the data storage tier. If a system cannot separate the associated database or other data storage components from the associated application, the system must be assigned to the application tier. This ensures that the effects of operating system or application errors or vulnerabilities on contiguous systems and databases are minimized.