

Technical Organizational Measures (TOMs)

Konzern-Datenschutz



|  |  |
| --- | --- |
|  |  |
| Technical Organizational Measures (TOMs) |  |
| Nummer | [Nummer] |
| Erlassen am | 12.06.2023 |
| Durch | Konzern-Datenschutzbeauftragter |
| Inkrafttreten | 12.06.2023 |
| Geltungsbereich | SÜDVERS Holding GmbH & Co. KG und deren Tochtergesellschaften mit Mehrheitsbeteiligung, sowie die SÜDVERS International GmbH |
| Geltungsbereich | SÜDVERS Gruppe |
| Thema | Compliance |
| Verantwortliche Funktion | Konzern-Datenschutz |
| Verantwortliche Person | Dirk Franken |
| Übergeordnete Vorschrift | SÜDVERS Datenschutzpolitik |
| Ersetzt | n/a |
| Mitgeltende Dokumente |  |
| Gültigkeit | Bis auf Widerruf |
| Letzte Überprüfung | 25.06.2025 |
| Nächste Überprüfung | 07.01.2026 |
| Publikation | SÜDVERS Intranet |
| Klassifizierung | Öffentlich |
| Archiv | Dokumentenverwaltungssystem |
| Ordnungssystem | [Ordnungssystem] |
| Sprachen | Englisch |
| Formate | Online |
| Bemerkungen |  |

The technical and organizational measures are implemented by SÜDVERS in accordance with Art 32 DSGVO. They are continuously improved by SÜDVERS according to feasibility and state of the art and brought to a higher level of security and protection.

Table of Content

[1 Confidentiality 4](#_Toc137448922)

[1.1 Physical Access Control 4](#_Toc137448923)

[1.2 Logical Access Control 5](#_Toc137448924)

[1.3 Authorization Control 6](#_Toc137448925)

[1.4 Separation Control 7](#_Toc137448926)

[1.5 Pseudonymization 8](#_Toc137448927)

[2 Integrity 9](#_Toc137448928)

[2.1 Transfer Control 9](#_Toc137448929)

[2.2 Input Control 10](#_Toc137448930)

[3 Availability and Resilience 11](#_Toc137448931)

[3.1 Availability Control 11](#_Toc137448932)

[3.2 Recoverability Control 12](#_Toc137448933)

[4 Procedures for regular Review, Assessment and Evaluation 13](#_Toc137448934)

[4.1 Data Protection Management 13](#_Toc137448935)

[4.2 Incident Response Management 14](#_Toc137448936)

[4.3 Data Protection by Design and by Default 15](#_Toc137448937)

[4.4 Order Control (outsourcing, subcontractors and order processing) 16](#_Toc137448938)

# Confidentiality

## Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Intruder alarm system | ☒ | Key regulation / List |
| ☒ | Automatic access control system | ☒ | Reception / Receptionist / Gatekeeper |
| ☒ | Smart cards / transponder systems | ☒ | Visitors' book / Visitors' protocol |
| ☒ | Manual locking system | ☒ | Visitor badges |
| ☒ | Doorbell system (with camera, where possible) | ☒ | Visitors accompanied by employees |
| ☒ | Video surveillance of entrances | ☒ | Care in selection of security guard personnel (data centers) |
| ☒ | Biometric access control data center | ☒ | Care in selection of cleaning services |
| ☐ |  | ☒ | Information Security Policy |
| ☐ |  | ☒ | Work instructions for operational safety |
| ☐ |  | ☒ | Work instruction access control |

## Logical Access Control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Login with individual user account + strong password | ☒ | Access control policy |
| ☒ | Anti-Virus Software Servers | ☒ | Central password assignment (Microsoft AD) |
| ☒ | Anti-Virus Software Clients | ☒ | Information Security Policy |
| ☒ | Anti-virus software mobile devices | ☒ | Work instruction IT user regulations |
| ☒ | Firewall | ☒ | Work instruction operational security |
| ☒ | Network based Intrusion Detection Systems | ☒ | Work instruction access control |
| ☒ | Host Based Intrusion Detection Systems | ☒ | Mobile Device Policy |
| ☒ | Use of VPN or Citrix for remote access | ☐ |  |
| ☒ | Encryption of portable electronic storage media | ☐ |  |
| ☒ | Encryption of smartphones | ☐ |  |
| ☒ | Automatic password protected screen saver | ☐ |  |
| ☒ | Encryption of notebooks / tablet | ☐ |  |
| ☒ | Two-factor authentication in data center operation and for critical systems | ☐ |  |

## Authorization 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.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | File shredder min. recommended security level P-4 (DIN 66399) | ☒ | Use of authorization concepts |
| ☒ | External destruction of files at least recommended security level P-6 (DIN 66399) | ☒ | Minimum number of administrators assigned |
| ☒ | Physical destruction of electronic storage media | ☒ | Management of user rights by administrators |
| ☒ | Logging of accesses to applications | ☒ | Information Security Policy |
| ☒ | SSH encrypted access (for externally accessible IT systems) | ☒ | Work instruction communication security |
| ☒ | Certified SSL encryption | ☒ | Work instruction Handling of classified information and IT systems |

## Separation Control

Measures that 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 | |
| ☒ | Separation of productive, test and development environments | ☒ | Control via authorization concept |
| ☒ | Physical separation (systems / databases / data carriers) | ☒ | Determination of database rights |
| ☒ | VLAN segmentation | ☒ | Information Security Policy |
| ☒ | Client systems logically separated | ☒ | Data Protection Policy |
| ☐ |  | ☒ | Work instruction operational security |
| ☐ |  | ☒ | Work instruction information security in software development |

## Pseudonymization

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 case of pseudonymization: handled as agreed in service contract | ☒ | Internal instruction to anonymize/ pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired |
| ☒ | log files are pseudonymized at the request of the client (currently not applicable as there is no customer access to systems) | ☒ | Information Security Policy |
| ☐ |  | ☒ | Data Protection Policy |
| ☐ |  | ☒ | Specific internal regulations on use of cryptography |

# Integrity

## Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Use of VPN | ☒ | Survey of regular retrieval and transmission processes |
| ☒ | Logging of accesses and retrievals | ☒ | Transmission in anonymized or pseudonymized form |
| ☒ | Provision via encrypted connections such as sftp, https, TLS | ☒ | Careful selection of transport personnel and vehicles (only applicable in case transport of physical storage media would be requested by customer) |
| ☒ | Use of signature procedures (case dependent and as agreed in service contract) | ☒ | In case transport of physical storage media would be requested, personal handover with protocol |
| ☐ |  | ☒ | Information Security Policy |
| ☐ |  | ☒ | Data Protection Policy |

## Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Technical logging of the entry, modification and deletion of data | ☒ | Survey of which programs can be used to enter, change or delete data |
| ☒ | Manual or automated control of the logs (according to strict internal specifications) | ☒ | Traceability of data entry, modification and deletion through individual user names (not user groups) |
| ☐ |  | ☒ | Assignment of rights to enter, change and delete data on the basis of an authorization concept |
| ☐ |  | ☒ | Retention of forms from which data has been transferred to automated processes |
| ☐ |  | ☒ | Clear responsibilities for deletions of personal data |
| ☐ |  | ☒ | Information Security Policy |
| ☐ |  | ☒ | Work instruction IT user regulations |

# Availability and Resilience

## Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Environment control systems (fire, water, …) | ☒ | Backup and Recovery concept |
| ☒ | Fire extinguisher server room | ☒ | No sanitary connections in the server room |
| ☒ | Server room monitoring (and alerting) of temperature and humidity | ☒ | Existence of an emergency plan |
| ☒ | Server room air-conditioning | ☒ | Storage of backup in a secure data center locations in >20km distance from the primary data center location |
| ☒ | UPS system and emergency power supply systems | ☒ | Separate partitions for operating systems and data where necessary |
| ☒ | Protective socket strips data center | ☒ | Information Security Policy |
| ☒ | Fault tolerant storage systems | ☒ | Work instruction operational security |
| ☒ | Video surveillance server room | ☒ | Regular testing of emergency power supplies |
| ☒ | Intruder alarm in case of unauthorized access to server room | ☐ |  |

## Recoverability Control

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Backup monitoring and reporting | ☒ | Backup and Recovery concept |
| ☒ | Restorability from automation tools | ☒ | Control of the backup process |
| ☒ | Backup concept according to criticality (based on BIA) and customer specifications | ☒ | Regular testing of data recovery and logging of results |
| ☐ |  | ☒ | Storage of backup in a secure data center locations in >20km distance from the primary data center location |
| ☐ |  | ☒ | BCP & DR plans |
| ☐ |  | ☒ | Information Security Policy |
| ☐ |  | ☒ | Work instruction operational security |

# Procedures for regular Review, Assessment and Evaluation

## Data Protection Management

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Central documentation of all data protection regulations with access for employees | ☒ | Group Data Protection Officer (DPO) appointed |
| ☒ | Information security framework based on international standards (ISO 27001 and ISO 27002, NIST CSF, ISF SoGP) | ☒ | Group Chief Information Security Officer appointed |
| ☒ | A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated | ☒ | Staff trained and obliged to confidentiality/data secrecy |
| ☒ | Data protection checkpoints consistently implemented in tool-supported risk assessment | ☒ | Regular awareness trainings at least annually |
| ☐ |  | ☒ | Data Protection Impact Assessment (DPIA) is carried out as required |
| ☐ |  | ☒ | Processes regarding information obligations according to Art 13 and 14 GDPR established |
| ☐ |  | ☒ | Formalized process for requests for information from data subjects is in place |
| ☐ |  | ☒ | Data protection aspects established as part of corporate risk management |
| ☐ |  | ☒ | ISO 27001 certification the company’s key IT service providers |

## Incident Response Management

Support for security breach response and data breach process.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Use of firewall and regular updating | ☒ | Documented process for detecting and reporting security incidents / data breaches (also with regards to reporting obligation to supervisory authority) |
| ☒ | Use of spam filter and regular updating | ☒ | Formalized procedure for handling security incidents (aligned with NIST SP800-61 rev. 2 and EU WP29 recommendations) |
| ☒ | Use of virus scanner and regular updating | ☒ | Involvement of CISO in security incidents and CISO and DPO in personal data breaches |
| ☒ | Network based Intrusion Prevention System (NIPS) | ☒ | Documentation of security incidents and personal data breaches via ticket system (process aligned with ITIL, NIST SP800-61 rev. 2 and EU WP 29 recommendations) |
| ☒ | Host based Intrusion Prevention System (HIPS) | ☒ | A formal process for following up on security incidents and personal data breaches (based on EU WP 29 recommendations) |
| ☒ | Anomaly detection systems | ☒ | Information Security Policy |
| ☐ |  | ☒ | Data Privacy Policy |
| ☐ |  | ☒ | Work instruction operational security |
| ☐ |  | ☒ | Work instruction IT user regulations |

## Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | No more personal data is collected than is necessary for the respective purpose | ☒ | Data Protection Policy (includes principles "privacy by design / by default") |
| ☒ | Use of data protection-friendly default settings in standard and individual software | ☐ | OWASP Secure Mobile Development Security Checks are performed.  (Currently not applicable as we do not develop software) |
| ☐ |  | ☒ | Perimeter analysis for web applications |

## Order Control (outsourcing, subcontractors and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the data subject’s or client's instructions.

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Measures | | Organizational Measures | |
| ☒ | Monitoring of remote access by external parties, e.g. in the context of remote support | ☒ | Work instruction supplier management and supplier evaluation |
| ☒ | Monitoring of subcontractors according to the principles and with the technologies according to the preceding chapters 1, 2 | ☒ | Prior review of the security measures taken by the contractor and their documentation |
| ☐ |  | ☒ | Selection of the contractor under due diligence aspects (especially with regards to data protection and information security) |
| ☐ |  | ☒ | Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses |
| ☐ |  | ☒ | Framework agreement on contractual data processing within the group of companies |
| ☐ |  | ☒ | Written instructions to the contractor |
| ☐ |  | ☒ | Obligation of the contractor's employees to maintain data secrecy |
| ☐ |  | ☒ | Agreement on effective control rights over the contractor |
| ☐ |  | ☒ | Regulation on the use of further subcontractors |
| ☐ |  | ☒ | Ensuring the destruction of data after termination of the contract |
| ☐ |  | ☒ | In the case of longer collaboration: ongoing review of the contractor and its level of compliance and protection |