

Guidance   
Contractual clauses

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Contractual clauses | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 17.01.2025 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Security Policy 3rd Party Service provider management | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of contents

[1 Clauses relating to general information security 4](#_Toc188367920)

[2 Clauses relating to information risk management 5](#_Toc188367921)

[3 Clauses relating to IT service management 6](#_Toc188367922)

[4 Compliance with best practice and manufacturer recommendations 6](#_Toc188367923)

[5 Clauses relating to audit 6](#_Toc188367924)

[6 Requirement for additional contract content in accordance with EU Regulation 2022/2554 Art. 30 7](#_Toc188367925)

[6.1 General requirements in accordance with EU Regulation 2022/2554 Art. 30 para. 2 7](#_Toc188367926)

[6.2 Additional requirements in accordance with EU Regulation 2022/2554 Art. 30 para. 3 8](#_Toc188367927)

[7 Additional clauses in the event that cloud computing is used 9](#_Toc188367928)

[8 Clauses relating to compliance with the PCI DSS 9](#_Toc188367929)

[9 Additional clauses in the event that the service is provided on a dedicated basis for SÜDVERS or SÜDVERS has direct or indirect operational responsibility for the service provided 10](#_Toc188367930)

[9.1 Change management 10](#_Toc188367931)

[9.2 Compliance with SÜDVERS standards and guidelines 10](#_Toc188367932)

[9.3 Changes to the SÜDVERS guidelines 10](#_Toc188367933)

This document describes the standard clauses that should be included by SÜDVERS in all contracts with third parties relating to the processing, storage or transfer of SÜDVERS data (including customer data).

Depending on the contract and the service to be provided, some of the chapters listed may be optional. In the event that not all clauses are to be applied, this must be agreed with the information security officer or the data protection officer for the respective individual case.

# Clauses relating to general information security

* <SERVICE PROVIDER> shall provide the service and operate the systems, whether certified or not, in accordance with industry recognized best practices in information security management, best practices for information security in technical operations and in accordance with all applicable vendor recommendations.

The following standards, norms, regulations, ... must be complied with as a minimum:

* + General Data Protection Regulation (GDPR)
  + REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience in the financial sector (DORA) and any related technical standards applicable to the service provider[[1]](#footnote-1)
  + ISO 27001ff
  + ISO 27036[[2]](#footnote-2)
  + ISO 27701
  + ISO 22301[[3]](#footnote-3)
  + ISAE 3402[[4]](#footnote-4)
* In the event that <DISCLOSURE MANAGER> or its subcontractors discover or are notified of a breach of security or potential breach of security, including any actual or potential illegal transmission of or access to SÜDVERS Data, <DISCLOSURE MANAGER> will promptly, but no later than within 3 hours for incidents that meet or may meet at least one (1) of the criteria for a Major Incident under DORA and within no more than 18 hours, notify <DISCLOSURE MANAGER> or its subcontractors of any breach of security or potential breach of security, including any actual or potential illegal transmission of or access to SÜDVERS Data
  + inform the SÜDVERS Information Security Officer of such a breach or potential breach, whereby the information provided must, to the extent known to the service provider, comply with the requirements of the relevant "Technical Standards with regards to the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat"
  + inform the IT Service Desk of SÜDVERS of such a breach or potential breach, whereby the information provided must, as far as known to the service provider, comply with the requirements of the relevant "Technical Standards with regards to the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat"
  + investigate the breach or potential breach and take all appropriate steps to prevent a recurrence of the breach or potential breach. < SERVICE PROVIDER> will not report the breach or potential breach to any governmental authority unless required to do so by applicable law. If such notification is required by applicable law, <service provider> will first consult with the SÜDVERS Information Security Officer.
* < SERVICE PROVIDER> undertakes to logically separate the SÜDVERS systems, data and information from the data and information of its other customers.
* < SERVICE PROVIDER> undertakes to set up and maintain separate and secure areas in its facilities for the provision of services to SÜDVERS. In the event that < SERVICE PROVIDER> uses non-dedicated environments to provide the Service to SÜDVERS, < SERVICE PROVIDER> must ensure that it is not technically possible to gain access to SÜDVERS systems or data from other customers using the same shared environment.
* < SERVICE PROVIDER> undertakes to comply with the DORA Regulation and its Technical Standards "use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554" and to provide evidence of compliance periodically (at least annually) if subcontractors are to be used for the fulfillment of the contract.

# Clauses relating to information risk management

* <SERVICE PROVIDER> shall have an information risk management system that complies with industry recognized best practices (such as ISO/IEC 27005 or others), whether certified or not, and shall follow industry best practices for operational risk management (as defined in ISO/IEC 27005, ISF IRAM2 or others) covering the entire system lifecycle of the service provided.
* <SERVICE PROVIDER> undertakes to have implemented an IT risk management system in accordance with REGULATION (EU) 2022/2554 Chapter II and the associated Technical Standards "ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554" and to demonstrate compliance periodically (at least annually).
* SERVICE PROVIDER> undertakes to apply IT risk management in accordance with REGULATION (EU) 2022/2554 Chapter II and the associated Technical Standards "ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554" to its subcontractors, insofar as these are used to provide the service for SÜDVERS.

# Clauses relating to IT service management

* < SERVICE PROVIDER> provides IT services in accordance with, whether certified or not, industry recognized best practices (such as ISO/IEC20000, ITIL or others) that cover the entire lifecycle of the service to be provided.
* < SERVICE PROVIDER> provides the Incident Management Service related to structure and roles and responsibilities according to NIST SP800-61 rev 2 (or newer).

# Compliance with best practice and manufacturer recommendations

* In providing the Services to SÜDVERS, <SUPPLIER> shall comply with best practice and manufacturer's recommendations in relation to the configuration, management, operation and development of a system, without limitation, subject to applicable laws and SÜDVERS standards, guidelines and policies.

# Clauses relating to audit

* The <SERVICE PROVIDER> shall provide SÜDVERS or a SÜDVERS representative with ten (10) days' notice access to such facilities, systems, records and documentation as may be reasonably requested by SÜDVERS to audit compliance with the obligations under this Agreement and shall cause its subcontractors to do so, systems, records and supporting documentation as may be reasonably requested by SÜDVERS to audit compliance with the <SERVICE PROVIDER>'s obligations under or in connection with this Agreement.SERVICE PROVIDER> under or in connection with this Agreement.
* The tests must be carried out in such a way that any interruption to the performance of <service provider> and other normal processes is kept to a minimum.
* If required by the regulatory authorities responsible for SÜDVERS, <DIENSTLEISTER> will cooperate with the regulatory authorities, including their auditors and examiners, in the same manner as provided in this section for audits conducted by SÜDVERS.
* SERVICE PROVIDER shall promptly provide SÜDVERS with full details of any breaches or process/system weaknesses mentioned in its internal audit reports or otherwise uncovered. Thereafter, <SERVICE PROVIDER> shall provide SÜDVERS with an acceptable plan for remediation of such violations and process/system weaknesses within thirty (30) days (unless a shorter period is required due to exigent circumstances) and thereafter diligently complete the remediation within said period.
* SÜDVERS, its auditors and other representatives will maintain reasonable confidentiality and security precautions and will not require access to <SÜDVERS> internal financial data (except in connection with the provision of services to SÜDVERS).
* <SERVICE PROVIDER> shall promptly provide SÜDVERS with the results (not the entire content, but only certain chapters) of any internal or external reviews or audits conducted by <SERVICE PROVIDER> and its internal and external auditors with respect to the operating practices and procedures of <DIENSTLEISTER> to the extent relevant to the Services provided to SÜDVERS and disclose any corrective actions taken and to be taken therein. SÜDVERS acknowledges that <DIENSTLEISTER>'s audit results and other related information are confidential information within the meaning of this Agreement.
* < SERVICE PROVIDER> is obliged to carry out ongoing internal and external penetration tests and vulnerability assessments of the virtual and physical infrastructure and services provided. The specific results of these reviews or audits will be discussed between <service provider> and SÜDVERS in quarterly meetings.

# Requirement for additional contract content in accordance with EU Regulation 2022/2554 Art. 30

## General requirements in accordance with EU Regulation 2022/2554 Art. 30 para. 2

The contractual agreements on the use of ICT services include at least the following elements:

* a clear and complete description of all functions and ICT services to be provided by the third-party ICT service provider, indicating whether subcontracting of IT services supporting critical or important functions or essential parts thereof is allowed and, if so, the conditions for such subcontracting;
* the locations (countries) where the contractually agreed or subcontracted functions and IT services are to be provided and where data is to be processed, including the storage location, as well as the requirement for the third-party IT service provider to notify the financial company in advance if it intends to change these locations;
* Provisions on availability, authenticity, integrity and confidentiality in relation to data protection, including the protection of personal data;
* Provisions on ensuring access to personal and non-personal data processed by the financial undertaking in the event of insolvency, liquidation, cessation of business by the third-party IT service provider or termination of the contractual agreements, and on the recovery and return of such data in an easily accessible format;
* Service level descriptions, including updates and revisions;
* the obligation of the third-party IT service provider to provide assistance to the financial undertaking in the event of an IT incident related to the ICT service provided to the financial undertaking, at no additional cost or at a cost to be determined in advance;
* the obligation of the third-party IT service provider to cooperate fully with the authorities and resolution authorities responsible for the financial undertaking, including the persons designated by them;
* Termination rights and related minimum notice periods for the termination of contractual agreements in accordance with the expectations of the competent authorities and the resolution authorities;
* Conditions for the participation of third-party IT service providers in the IT security awareness and digital operational resilience training programs offered by financial undertakings in accordance with Article 13(6).

## Additional requirements in accordance with EU Regulation 2022/2554 Art. 30 para. 3

The contractual arrangements for the use of IT services to support critical or important functions (corresponding to a criticality of the service providers of level "medium" or higher or higher according to BIA) shall include at least the following elements in addition to those mentioned in the previous paragraph:

* complete service level descriptions, including updates and revisions, with precise quantitative and qualitative performance targets within the agreed service level to enable the finance company to effectively monitor IT services and take appropriate corrective action without delay if an agreed service level is not achieved;
* notice periods and reporting obligations of the third-party IT service provider to the financial undertaking, including reporting any developments that could materially impact the ability of the third-party IT service provider to effectively provide IT services in support of critical or important functions in accordance with the agreed performance levels;
* Requirements for the third-party IT service provider to implement and test contingency plans and to have measures, tools and IT security policies and guidelines in place that provide an appropriate level of security for the provision of services by the financial undertaking in accordance with its legal framework;
* the obligation of the third party IT service provider to participate and cooperate fully in the TLPT of the financial undertaking referred to in Articles 26 and 27;
* the right to monitor the performance of the third-party IT service provider on an ongoing basis, which includes: L 333/52 EN Official Journal of the European Union 27.12.2022
  + unrestricted access, inspection and audit rights of the financial undertaking or a delegated third party and the competent authority as well as the right to obtain copies of relevant documents on site if they are of decisive importance for the business activities of the IT third-party service provider, whereby the actual exercise of these rights is not hindered or restricted by other contractual agreements or implementation guidelines;
  + the right to agree alternative confirmation levels if the rights of other customers are affected;
  + the obligation of the third-party IT service provider to cooperate fully with on-site inspections and audits carried out by the competent authorities, the lead supervisory authority, the financial undertaking or a delegated third party; and iv) the obligation to provide details of the scope and frequency of such inspections and the procedure to be followed;

# Additional clauses in the event that cloud computing is used

* < SERVICE PROVIDER> shall provide the service and operate the systems in accordance with ISO/IEC 27017 and ISO/IEC 27018, regardless of whether they are certified or not.
* < SERVICE PROVIDER> must protect SÜDVERS' information by meeting at least the following requirements
  + Provide a secure, strong authentication service (whenever possible, single sign-on using AD integration or federated services must be used),
  + Restrict access to authorized users,
  + Restriction of access to cloud services if the connections originate from outside the SÜDVERS corporate firewall,
  + Management of access controls of the cloud service to meet the requirements of SÜDVERS,
  + the implementation of suitable solutions for monitoring and protection against malware,
  + the implementation of suitable solutions for attack detection (active network-based IPS) at the network perimeter of the services provided, and
  + Provision of a method for the secure destruction of SÜDVERS information stored in the cloud as soon as it is no longer required.
* < SERVICE PROVIDER> must request a declaration of consent from SÜDVERS prior to any change in the way the service is delivered to SÜDVERS if the following measures are planned:
  + Relocation of the technical IT infrastructure to another geographical region (country) or another jurisdiction,
  + the processing or storage of information in a new geographical region (country) or jurisdiction

# Clauses relating to compliance with the PCI DSS

* For all processes, procedures or systems that fall within the scope of PCI DSS, <DIENSTLEISTER> must comply with PCI DSS 4.0 (or later) in relation to the configuration, management, operation and development of the services provided to SÜDVERS

# Additional clauses in the event that the service is provided on a dedicated basis for SÜDVERS or SÜDVERS has direct or indirect operational responsibility for the service provided

## Change management

* SÜDVERS has a right to approve any changes that could adversely affect the receipt or use of the Services, increase <DIENSTLEISTER>'s fees or other costs to SÜDVERS, or have a negative impact on the security of the system and/or the information stored, processed or transmitted or the reputation of SÜDVERS.
* < SERVICE PROVIDER> shall not be obliged to comply with change requests from SÜDVERS if compliance with such requests would violate applicable law. In this case, the <SERVICE PROVIDER> shall inform SÜDVERS immediately and provide a statement to this effect.

## Compliance with SÜDVERS standards and guidelines

In providing the Services to SÜDVERS, <SUPPLIER> shall comply with SÜDVERS' applicable standards, guidelines and policies, including but not limited to those developed, amended and communicated to <SUPPLIER> in writing from time to time by SÜDVERS ("SÜDVERS Policies"), subject to applicable law.

## Changes to the SÜDVERS guidelines

* SÜDVERS shall bear the costs associated with the <SUPPLIER's> compliance with changes to the SÜDVERS Policies, unless the changes to the SÜDVERS Policies are made to reflect the requirements of applicable law or changes related to changes in best practices.
* < SERVICE PROVIDER> must request consent from SÜDVERS before making any changes to the way the Service is provided to SÜDVERS, including:
  + Changes to the technical IT infrastructure (e.g. major upgrades to operating systems or application software or a significant reconfiguration of systems such as virtual servers or storage networks),
  + the reconfiguration of cloud services, or
  + the use of other external parties (e.g. the change or use of new subcontractors to support the provision of services).

1. Only relevant for DORA level 1 IT service providers (direct contractual relationship) and for all other IT service providers in the supply chain if they provide important or critical IT servicesb [↑](#footnote-ref-1)
2. Only relevant for IT service providers with operational responsibility [↑](#footnote-ref-2)
3. Only relevant for IT service providers with operational responsibility [↑](#footnote-ref-3)
4. Only relevant for IT service providers with operational responsibility or with access to SÜDVERS business information [↑](#footnote-ref-4)