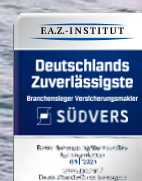



Versicherungs- und Risikomanagement  
Kredit- und Bürgschaftsmanagement  
SÜDVERS International  
D&O und Cyber  
Vorsorge, Pension & Employee Benefits



## Group Data Privacy

## Data Privacy Policy




Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## Data Privacy Policy

Issued on	21.06.2022
Issued by	Group Data Privacy Officer
Effective date	21.06.2022
Area of applicability	SÜDVERS Group
Topic	Compliance
Responsible function	Group Data Privacy
Responsible person	Nina Hartmann
Overriding provision	None
This document replaces	n/a
Valid until	Until revoked
Last review	17.07.2023
Next Review	08.01.2024
Publication	SÜDVERS Intranet
Classification	Public
Archive	d3
Language	English
Format	Online
Remarks	

## Table of Content

1	Principles for processing personal data .....	4
1.1	Fairness and lawfulness .....	4
1.2	Restriction to a specific purpose .....	4
1.3	Transparency .....	4
1.4	Data reduction and data economy .....	4
1.5	Deletion .....	5
1.6	Factual accuracy; up-to-dateness of data .....	5
1.7	Confidentiality and data security .....	5
2	Reliability of data processing.....	6
3	Customer and partner data .....	7
3.1	Data processing for a contractual relationship .....	7
3.2	Data processing for advertising purposes.....	7
3.3	Consent to data processing.....	7
3.4	Data processing pursuant to legal authorization .....	7
3.5	Data processing pursuant to legitimate interest .....	8
3.6	Processing of highly sensitive data .....	8
3.7	Automated individual decisions .....	8
3.8	User data and internet .....	8
4	Employee data .....	9
4.1	Data processing for the employment relationship .....	9
4.2	Data processing pursuant to legal authorization .....	9
4.3	Collective agreements on data processing .....	9
4.4	Consent to data processing.....	9
4.5	Data processing pursuant to legitimate interest .....	10
4.6	Processing of highly sensitive data .....	10
4.7	Automated decisions.....	10
4.8	Telecommunications and internet .....	11
5	Transmission of personal data .....	12
6	Contract data processing.....	13
7	Rights of the data subject.....	14
8	Confidentiality of processing.....	15
9	Processing security .....	16
10	Data protection control.....	17
11	Data protection incidents.....	18

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

As part of its responsibility, SÜDVERS is committed to international compliance with data protection SÜDVERS. This information privacy policy applies worldwide to SÜDVERS and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of SÜDVERS as an attractive employer. This policy provides one of the necessary framework conditions for cross-border data transfer amongst SÜDVERS legal entities as well as between SÜDVERS and 3<sup>rd</sup> parties. It ensures the adequate level of data protection prescribed by the *General Data Protection Regulation (GDPR)* (EU) 2016/679 and the national SÜDVERS for cross-border data transfer, including in countries that do not yet have adequate data protection SÜDVERS.

## 1 Principles for processing personal data

### 1.1 Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

### 1.2 Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.


### 1.3 Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

- The identity of the Data Controller
- The purpose of data processing
- Third parties or categories of third parties to whom the data might be transmitted

### 1.4 Data reduction and data economy

Before processing personal data, SÜDVERS will determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

### 1.5 Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods will be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.


### 1.6 Factual accuracy; up-to-dateness of data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps will be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

### 1.7 Confidentiality and data security


Personal data is subject to data protection. It must be treated as confidential on a personal level and secured with appropriate and best practice oriented organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.



Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 2 Reliability of data processing

Storing, processing and transmitting personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of storing, processing and transmitting the personal data is to be changed from the original purpose.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

### 3 Customer and partner data

#### 3.1 Data processing for a contractual relationship

Personal data of customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfil other requests that relate to contract conclusion. Related people can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the related people will be complied with.

#### 3.2 Data processing for advertising purposes


If the data subject contacts SÜDVERS to request information (such as request to receive information material about a product), data processing to meet this request is permitted. Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone. If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and will be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes will be observed.

#### 3.3 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with this policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

#### 3.4 Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

### 3.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of SÜDVERS. Legitimate interests are generally of a legal (such as collection of outstanding receivables) or commercial nature (such as avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

### 3.6 Processing of highly sensitive data

Sensitive personal data can be processed only if the law requires this or the data subject has given explicit consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process sensitive data, the SÜDVERS Data Protection Officer will be informed in advance.


### 3.7 Automated individual decisions

Automated processing of personal data that might under some circumstances be used to evaluate certain aspects will not be used as the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject will be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check will always be made by an employee.

### 3.8 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects. If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be affected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement. If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.



Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 4 Employee data

### 4.1 Data processing for the employment relationship

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application between SÜDVERS legal entities. In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national SÜDVERS have to be observed. In cases of doubt, consent must be obtained from the data subject. There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of SÜDVERS.

### 4.2 Data processing pursuant to legal authorization


The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

### 4.3 Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

### 4.4 Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national SÜDVERS do not require express consent. Before giving consent, the data subject must be informed in accordance with this policy.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

#### 4.5 Data processing pursuant to legitimate interest


Personal data can also be processed if it is necessary to enforce a legitimate interest of SÜDVERS. Legitimate interests are generally of a legal (such as filing, enforcing or defending against legal claims) or financial (such as valuation of companies) nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (such as compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (such as rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

#### 4.6 Processing of highly sensitive data

Highly sensitive personal data can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. Moreover, data that relates to a crime (such as theft of SÜDVERS properties) can often be processed only under special requirements under national law. The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in the area of employment law. The employee can also expressly consent to processing. If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.


#### 4.7 Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (such as as part of personnel selection or the evaluation of skills profiles), this automatic processing will not be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process will ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

#### 4.8 Telecommunications and internet


Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal SÜDVERS policies. In the event of authorized use for private purposes, the SÜDVERS on secrecy of telecommunications and the relevant national telecommunication SÜDVERS must be observed, if applicable. There will be no general monitoring of telephone and email communications or internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented to protect the security of SÜDVERS. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of SÜDVERS or policies of SÜDVERS. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national SÜDVERS must be observed in the same manner as the SÜDVERS policies.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 5 Transmission of personal data

Transmission of personal data to recipients outside or inside SÜDVERS is subject to the authorization requirements for processing personal data. The data recipient must be required to use the data only for the defined purposes. In the event that data is transmitted to a recipient outside SÜDVERS to a third country this country must agree to maintain a data protection level equivalent to this data privacy policy. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the SÜDVERS of the domiciliary country of the SÜDVERS legal entity transmitting the data. In the alternative, the SÜDVERS of the domiciliary country of the SÜDVERS legal entity can acknowledge the purpose of data transmission based on the legal obligation of a third country. If data is transmitted by a third party to SÜDVERS, it must be ensured that the data can be used for the intended purpose. If personal data is transferred from an SÜDVERS legal entity with its registered office in the European Union/European Economic Area to an SÜDVERS legal entity with its registered office outside of the European Economic Area (third country), the company importing the data is obligated to cooperate with any inquiries made by the relevant supervisory authority in the country in which the party exporting the data has its registered office, and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data. The same applies to data transmission by SÜDVERS legal entities from other countries.


In the event that a data subject claims that this data privacy policy has been breached by an SÜDVERS entity located in a third country that is importing the data, the SÜDVERS entity located in the European Economic Area that is exporting the data undertakes to support the party concerned, whose data was collected in the European Economic Area, in establishing the facts of the matter and also asserting his/her rights in accordance with this policy against the SÜDVERS legal entity importing the data. In addition, the data subject is also entitled to assert his or her rights against the SÜDVERS legal entity exporting the data. In the event of claims of a violation, the company exporting the data must document to the data subject that the company importing the data in a third country (in the event that the data is further processed after receipt) did not violate this data privacy policy. In the case of personal data being transmitted from an SÜDVERS legal entity located in the European Economic Area to an SÜDVERS legal entity located in a third country, the data controller transmitting the data shall be held liable for any violations of this policy committed by the SÜDVERS legal entity located in a third country with regard to the data subject whose data was collected in the European Economic Area, as if the violation had been committed by the data controller transmitting the data. The legal venue is the responsible court where the company exporting the data is located.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 6 Contract data processing

Data processing on behalf means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on data processing on behalf must be concluded with external providers and among companies within SÜDVERS. The client retains full responsibility for correct performance of data processing. The provider can process personal data only as per the instructions from the client. When issuing the order, the following requirements must be complied with:

- The provider must be chosen based on its ability to cover the required technical and organizational protective measures.
- The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.
- The contractual standards for data protection provided by the SÜDVERS Data Protection Officer must be considered.
- Before data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.
- In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from the European Economic Area can be processed in a third country only if the provider can prove that it has a data protection standard equivalent to this data privacy policy. Suitable tools can be:
  - Agreement on EU standard contract clauses for contract data processing in third countries with the provider and any subcontractors.
  - Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.
  - Acknowledgment of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.


Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 7 Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.


- The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (such as personnel file) for the employment relationship under the relevant employment SÜDVERS, these will remain unaffected.
- If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.
- If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
- The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.
- The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
- The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.



Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	


## 8 Confidentiality of processing

Personal data is subject to data confidentiality. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Line managers must inform their employees at the start of the employment relationship about the obligation to protect data confidentiality. This obligation shall remain in force even after employment has ended.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	


## 9 Processing security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). In particular, the responsible department can consult the SÜDVERS Chief Information Security Officer. The technical and organizational measures for protecting personal data are part of information security management and must be adjusted continuously to the technical developments and organizational changes.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 10 Data protection control

Compliance with the data privacy policy and the applicable data protection SÜDVERS is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Officer and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the Data Protection Officer. The SÜDVERS Board of Directors must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

Version: 1.0	Group Data Privacy	
21.06.2022	Data Privacy Policy	

## 11 Data protection incidents

All employees must inform their supervisor or Data Protection Officer immediately about cases of violations against this data privacy policy or other regulations on the protection of personal data (data protection incidents). The manager responsible for the function or the unit is required to inform the Data Protection Officer immediately about data protection incidents.

In cases of

- improper transmission of personal data to third parties,
- improper access by third parties to personal data, or
- loss of personal data

the required legal entity has to report the incident immediately so that any reporting duties under national law can be complied with.