

Data privacy policy

Group Data Privacy

|  |  |
| --- | --- |
|  |  |
| Data protection policy |  |
| Number | [Number] |
| Issued on | 21.06.2022 |
| Through | Group Data Privacy Officer |
| Entry into force | 21.06.2022 |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH |
| Topic | Compliance |
| Responsible function | Group Data Privacy |
| Responsible person | Udo Strittmatter |
| Overriding regulation | [Parent regulation] |
| Replaces | n/a |
| Applicable documents |  |
| Validity | Until further notice |
| Last | 25.06.2025 |
| Next review | 07.01.2026 |
| Publication | SÜDVERS Intranet |
| Classification | Public |
| Archive | Document management system |
| Organizational system | [Organizational system] |
| Languages | English |
| Formats | Online |
| Remarks |  |

Table of contents

[1 Principles for the processing of personal data 4](#_Toc187665866)

[1.1 Fairness and legality 4](#_Toc187665867)

[1.2 Restriction to a specific purpose 4](#_Toc187665868)

[1.3 Transparency 4](#_Toc187665869)

[1.4 Data reduction and data economy 5](#_Toc187665870)

[1.5 Deletion 5](#_Toc187665871)

[1.6 Factual accuracy; topicality of the data 5](#_Toc187665872)

[1.7 Confidentiality and data security 5](#_Toc187665873)

[1.8 Reliability of data processing 5](#_Toc187665874)

[2 Customer and partner data 6](#_Toc187665875)

[2.1 Data processing within the framework of a contractual relationship 6](#_Toc187665876)

[2.2 Data processing for advertising purposes 6](#_Toc187665877)

[2.3 Consent to data processing 6](#_Toc187665878)

[2.4 Data processing based on a legal authorization 7](#_Toc187665879)

[2.5 Data processing on the basis of a legitimate interest 7](#_Toc187665880)

[2.6 Processing of highly sensitive data 7](#_Toc187665881)

[2.7 Automated individual decisions 7](#_Toc187665882)

[2.8 User data and Internet 7](#_Toc187665883)

[3 Employee data 8](#_Toc187665884)

[3.1 Data processing for the employment relationship 8](#_Toc187665885)

[3.2 Data processing based on a legal authorization 8](#_Toc187665886)

[3.3 Collective agreements on data processing 9](#_Toc187665887)

[3.4 Consent to data processing 9](#_Toc187665888)

[3.5 Data processing on the basis of a legitimate interest 9](#_Toc187665889)

[3.6 Processing of highly sensitive data 10](#_Toc187665890)

[3.7 Automated decisions 10](#_Toc187665891)

[3.8 Telecommunications and Internet 10](#_Toc187665892)

[3.9 Transmission of personal data 11](#_Toc187665893)

[4 Order data processing 12](#_Toc187665894)

[5 Rights of the data subject 13](#_Toc187665895)

[6 Confidentiality of the processing 13](#_Toc187665896)

[7 Processing safety 14](#_Toc187665897)

[8 Control of data protection 14](#_Toc187665898)

[9 Incidents in connection with data protection 14](#_Toc187665899)

SÜDVERS is committed to international compliance with data protection laws as part of its responsibility. This data protection policy applies to SÜDVERS worldwide and is based on

globally recognized, fundamental principles of data protection. The guarantee of data protection is the basis for trusting business relationships and the reputation of SÜDVERS as an attractive employer. This policy forms one of the necessary frameworks for the cross-border transfer of data between SÜDVERS business units and between SÜDVERS and 3rd parties. It ensures the adequate level of data protection required by the General Data Protection Regulation (GDPR) (EU) 2016/679 and national laws for cross-border data transfers and also applies to SÜDVERS in countries that do not yet have adequate data protection laws.

# Principles for the processing of personal data

## Fairness and legality

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

## Restriction to a specific purpose

Personal data may only be processed 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 justification.

## Transparency

The data subject must be informed about how their data will be processed. In general, personal data must be collected directly from the data subject.

If the data is collected, the data subject must either be aware of it or be informed of it:

* The identity of the data controller
* The purpose of data processing
* Third parties or categories of third parties to whom the data may be transferred

## Data reduction and data economy

Before processing personal data, SÜDVERS checks whether and to what extent the processing is necessary.

personal data is necessary to achieve the purpose for which it was collected.

If the purpose permits and the effort involved is proportionate to the objective pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for possible future purposes, unless this is required or permitted under national law.

## Deletion

Personal data that is no longer required after the expiry of legal or business process-related deadlines will be deleted. In individual cases, there may be an indication of interests worthy of protection or the historical significance of this data. In this case, the data must be retained until the interests worthy of protection have been legally clarified or the company archive has evaluated the data to determine whether it must be retained for historical purposes.

## Factual accuracy; topicality of the data

The personal data stored must be correct and complete and - if necessary updated. Appropriate measures are taken to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

## Confidentiality and data security

Personal data is subject to data protection. It must be kept confidential at a personal level and secured by appropriate and best practice organizational and technical measures to prevent unauthorized access, unlawful processing or dissemination and accidental loss, alteration or destruction.

## Reliability of data processing

The storage, processing and transfer of personal data is only permitted on the following legal bases. One of these legal bases is also required if the purpose of the storage, processing and transfer of personal data is to be changed from the original purpose.

# Customer and partner data

## Data processing within the framework of a contractual relationship

Personal data of customers and partners may be processed for the establishment, execution and termination of a contract. This also includes advising the partner as part of the contract, if this is related to the purpose of the contract. In the run-up to a contract - in the contract initiation phase - personal data may be processed in order to prepare offers or orders or to fulfill other requests related to the conclusion of the contract. The data subjects may be contacted during the contract preparation phase on the basis of the information they provide. All restrictions requested by the data subjects are observed.

## Data processing for advertising purposes

If the data subject contacts SÜDVERS to request information (e.g. request for information material on a product), data processing is permitted to fulfill this request. Further legal requirements apply to customer loyalty or advertising measures. Personal data may be processed for the purposes of advertising or market and opinion research, provided this is compatible with the purpose for which the data was originally collected. The data subject must be informed about the use of their data for advertising purposes. If data is only collected for advertising purposes, disclosure by the data subject is voluntary. The data subject must be informed that the provision of data for this purpose is voluntary. When communicating with the data subject, their consent to the processing of data for advertising purposes is obtained. When giving consent, the data subject should be given the opportunity to choose between the available forms of contact such as post, e-mail and telephone. If the data subject refuses the use of their data for advertising purposes, it can no longer be used for these purposes and will be blocked for use for these purposes. Other country-specific restrictions on the use of data for advertising purposes are observed.

## Consent to data processing

The data may be processed with the consent of the data subject. Before consent is given, the data subject must be informed in accordance with this policy. The declaration of consent must be obtained in writing or electronically for documentation purposes. In certain circumstances, e.g. in the case of telephone conversations, consent may also be given verbally. The granting of consent must be documented.

## Data processing on the basis of a legal authorization

The processing of personal data is also permitted if this is required, prescribed or permitted by national legislation. The type and scope of data processing must be necessary for the legally permissible data processing activity and comply with the relevant legal provisions.

## Data processing based on a legitimate interest

Personal data may also be processed if this is necessary for a legitimate interest of SÜDVERS. Legitimate interests are generally of a legal (e.g. collection of outstanding claims) or economic nature (e.g. avoidance of breaches of contract). Personal data may not be processed to safeguard a legitimate interest if, in individual cases, there are indications that the interests of the data subject worthy of protection prevail. Before processing data, it must be checked whether there are interests worthy of protection.

## Processing of highly sensitive data

Sensitive personal data may only be processed if this is required by law or if the data subject has expressly consented. This data may also be processed if this is necessary for the assertion, exercise or defense of legal claims of the data subject. If the processing of sensitive data is planned, the SÜDVERS data protection officer will be informed in advance.

## Automated individual decisions

Automated processing of personal data, which may be used to evaluate certain aspects, is not used as the sole basis for decisions that could have negative legal consequences or significantly affect the data subject. The data subject is informed of the facts and the results of automated individual decisions and is given the opportunity to respond. In order to avoid incorrect decisions, a test and plausibility check is always carried out by an employee.

## User data and Internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed about this in a privacy policy and, if applicable, in information about cookies. The privacy policy and any cookie information must be integrated in such a way that they are easily recognizable, directly accessible and consistently available to the data subjects. If usage profiles (tracking) are created in order to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy policy . Personal tracking may only take place if it is permitted under national law or with the consent of the data subject. If a pseudonym is used for tracking, the data subject should be given the opportunity to opt out in the privacy policy. If websites or apps can access personal data in an area reserved for registered users, the identification and authentication of the data subject must offer sufficient protection during access.

# Employee data

## Data processing for the employment relationship

Personal data may be processed in employment relationships if this is necessary for the initiation, implementation and termination of the employment relationship. Applicants' personal data may be processed when an employment relationship is initiated. If the applicant is rejected, their data must be deleted in compliance with the prescribed retention period, unless the applicant has consented to remain on file for a future selection procedure. Consent is also required in order to use the data for further application procedures or before the application is passed on between the SÜDVERS legal entities. In the existing employment relationship, data processing must always relate to the purpose of the employment contract if none of the following circumstances exist for permissible data processing. If it is necessary to obtain information about an applicant from a third party as part of the application process, the requirements of the relevant national laws must be observed. In case of doubt, the consent of the data subject must be obtained. There must be a legal authorization for the processing of personal data that is related to the employment relationship but was not originally part of the fulfillment of the employment contract. This can be statutory provisions, collective regulations with the employee representatives, the consent of the employee or the legitimate interest of SÜDVERS.

## Data processing on the basis of a legal authorization

The processing of personal employee data is also permitted if this is required, prescribed or permitted by national legislation. The type and scope of data processing must be necessary for the legally permitted data processing activity and comply with the relevant statutory provisions. If there is legal leeway, the employee's interests worthy of protection must be taken into account.

## Collective agreements on data processing

If a data processing activity goes beyond the purpose of fulfilling the contract, it may be permissible if it is authorized by a collective agreement. The agreements must relate to the specific purpose of the intended data processing activity and be drawn up within the framework of national data protection regulations.

## Consent to data processing

Employee data can be processed with the consent of the data subject. Declarations of consent must be given voluntarily. Involuntary consent is invalid. The declaration of consent must be obtained in writing or electronically for documentation purposes. In certain circumstances, consent may also be given verbally, in which case it must be properly documented. In the case of informed, voluntary provision of data by the data subject, consent can be assumed if national legislation does not require explicit consent. Before consent is given, the data subject must be informed in accordance with this Directive.

## Data processing based on a legitimate interest

Personal data may also be processed if this is necessary to enforce a legitimate interest of SÜDVERS. Legitimate interests are generally of a legal (e.g. assertion, enforcement or defense of legal claims) or economic (e.g. valuation of companies) nature. Personal data may not be processed on the basis of a legitimate interest if there are indications in individual cases that the employee's interests are worthy of protection. Before processing data, it must be checked whether there is an interest worthy of protection. Control measures that require the processing of employee data can only be taken if there is a legal obligation to do so or if there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must be examined. The legitimate interests of the company in carrying out the control measure (e.g. compliance with statutory provisions and internal company regulations) must be weighed against the legitimate interests of the employee affected by the measure in its exclusion and may only be carried out if they are reasonable. The legitimate interests of the company and the interests of the employee worthy of protection must be determined and documented prior to the measure. Furthermore, any additional requirements under national law (e.g. co-determination rights of employee representatives and information rights of those affected) must be taken into account.

## Processing of highly sensitive data

Highly sensitive personal data may only be processed under certain conditions. Highly sensitive data are data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the health and sex life of the data subject. Under national law, further categories of data may be classified as highly sensitive or the content of the data categories may be filled in differently. In addition, data relating to a criminal offense (e.g. theft of SÜDVERS property) can often only be processed under special conditions under national law. Processing must be expressly permitted or required under national law. In addition, processing may be permitted if it is necessary for the competent authority to fulfill its rights and obligations in the area of labor law. The employee can also expressly consent to the processing. If the processing of highly sensitive data is planned, the data protection officer must be informed in advance.

## Automated decisions

If personal data is processed automatically in the context of the employment relationship and certain personal data is evaluated (e.g. in the context of personnel selection or the evaluation of skills profiles), this automated processing must not be the sole basis for decisions that would have negative consequences or significant problems for the employee concerned. In order to avoid wrong decisions, the automated process must ensure that a natural person assesses the content of the situation and that this assessment is the basis for the decision. The data subject must also be informed of the facts and the results of automated individual decisions and have the opportunity to react to them.

## Telecommunications and Internet

Telephone systems, e-mail addresses, intranet and internet as well as internal social networks are primarily provided by the company for work-related tasks. They are a tool and a company resource. They can be used within the framework of the applicable legal provisions and internal SÜDVERS guidelines. In the case of authorized use for private purposes, the laws on telecommunications secrecy and the respective national telecommunications laws must be observed where applicable. There is no general monitoring of telephone and e-mail communication or Internet use. To defend against attacks on the IT infrastructure or individual users, protective measures may be taken to protect the security of SÜDVERS. For security reasons, the use of telephone systems, e-mail addresses, intranet/internet and internal social networks may be logged for a limited period of time.

Evaluations of this data of a specific person can only be carried out in a concrete, justified case of suspicion of violations of laws or guidelines of SÜDVERS. The evaluations may only be carried out by investigating bodies in compliance with the principle of proportionality. The relevant national laws must be observed in the same way as the SÜDVERS guidelines.

## Transmission of personal data

The transfer of personal data to recipients outside or within SÜDVERS is subject to the authorization requirements for the processing of personal data. The data recipient must be obliged to use the data only for the specified purposes. If data is transferred to a recipient outside SÜDVERS in a third country, this country must undertake to comply with a level of data protection that corresponds to this data protection declaration. This does not apply if the transfer is based on a legal obligation. Such a legal obligation may arise from the law of the country of domicile of the SÜDVERS legal entity transferring the data. Alternatively, the law of the country of domicile of the SÜDVERS business unit may recognize the purpose of the data transfer based on the legal obligation of a third country. If data is transferred to SÜDVERS by a third party, it must be ensured that the data can be used for the intended purpose. If personal data is transferred from a SÜDVERS business unit based in the European Union/European Economic Area to a SÜDVERS business unit based outside the European Economic Area (third country), the data-importing company is obliged to cooperate with requests from the competent supervisory authority of the country in which the data-exporting party is based and to comply with any findings of the supervisory authority regarding the processing of the transferred data. The same applies to the transfer of data by SÜDVERS business units from other countries.

In the event that a data subject alleges a breach of this Privacy Policy by a data-importing SÜDVERS entity based in a third country, the data-exporting SÜDVERS entity based in the European Economic Area undertakes to assist the data subject whose data was collected in the European Economic Area in establishing the facts and asserting his or her rights under this Privacy Policy also against the data-importing SÜDVERS entity. In addition, the data subject is also entitled to assert their rights against the data-exporting legal entity of SÜDVERS. In the event of an assertion of a violation, the data-exporting company must document to the data subject that the data-importing company in a third country (in the case of further processing of the data after receipt) has not violated this privacy policy. If personal data is transferred from a SÜDVERS business unit located in the European Economic Area to a SÜDVERS business unit located in a third country, the business unit transferring the data shall be liable for any breach of this Privacy Policy by the SÜDVERS business unit located in a third country vis-à-vis the data subject whose data was collected in the European Economic Area as if the breach had been committed by the business unit transferring the data. The place of jurisdiction is the competent court at the registered office of the company exporting the data.

# Order data processing

Data processing on behalf means that a provider is commissioned to process personal data without being given responsibility for the corresponding business process. In these cases, an agreement on commissioned data processing must be concluded with external providers and between companies within SÜDVERS. The client bears full responsibility for the proper execution of data processing. The provider may only process personal data in accordance with the client's instructions. The following requirements must be observed when placing an order:

* The provider must be selected on the basis of whether it is able to cover the necessary technical and organizational protective measures.
* The order must be placed in writing. The instructions for data processing and the responsibilities of the client and provider must be documented.
* The contractual specifications of the SÜDVERS data protection officer regarding data protection must be observed.
* The customer must be able to rely on the provider's compliance with the obligations before data processing begins. A provider can document compliance with the data security requirements in particular by presenting suitable certificates. Depending on the risk of data processing, the checks must be repeated regularly during the term of the contract.
* In the case of cross-border commissioned data processing, the respective national requirements for the transfer of personal data abroad must be met. In particular, personal data from the European Economic Area may only be processed in a third country if the provider can demonstrate a data protection standard equivalent to this privacy policy. Suitable tools can be:
  + Agreement of EU standard contractual clauses for commissioned data processing in third countries with the provider and any subcontractors.
  + Participation of the provider in an EU-accredited certification system to ensure an adequate level of data protection.
  + Recognition of binding corporate rules of the provider to create an appropriate level of data protection by the competent supervisory authorities for data protection.

# Rights of the data subject

Every data subject has the following rights, the assertion of which must be processed immediately by the responsible body and must not be detrimental to the data subject.

* The data subject may request information about what personal data is stored about them, how the data was collected and for what purpose. If further rights to inspect the employer's documents (e.g. personnel file) for the employment relationship exist under the relevant labor law regulations, these remain unaffected.
* If personal data is disclosed to third parties, the identity of the recipient or categories of recipients must be specified.
* If personal data is incorrect or incomplete, the data subject may request that it be corrected or completed.
* The data subject may object to the processing of their data for the purposes of advertising or market/opinion research. The data must be blocked for these types of use.
* The data subject may request the erasure of their data if there is no legal basis for the processing of this data or the legal basis has ceased to exist. The same applies if the purpose of the data processing has ceased to apply or no longer applies for other reasons. Existing retention periods and conflicting interests worthy of protection must be observed.
* In principle, the data subject has a right to object to the processing of their data, which must be taken into account if the protection of their interests outweighs the interests of the controller due to a particular personal situation. This does not apply if a legal provision prescribes the processing of the data.

# Confidentiality of the processing

Personal data is subject to data secrecy. Any unauthorized collection, processing or use of such data by employees is prohibited. Any data processing by an employee who is not authorized to do so as part of their legitimate duties is prohibited. The "need to know" principle applies. Employees may only have access to personal data to the extent that is appropriate for the type and scope of the respective task. This requires a careful division, separation and implementation of roles and responsibilities. Employees are prohibited from using personal data for private or commercial purposes, passing it on to unauthorized persons or making it accessible in any other way. Supervisors must inform their employees of the obligation to maintain data confidentiality at the beginning of the employment relationship. This obligation remains in force even after termination of the employment relationship.

# Processing safety

Personal data must be protected against unauthorized access and unlawful processing or disclosure and against accidental loss, alteration or destruction. This applies regardless of whether the data is processed electronically or in paper form. Before introducing new methods of data processing, in particular new IT systems, technical and organizational measures for the protection of 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 for protection of the data (determined by the information classification procedure). The responsible body may in particular consult the information security officer of SÜDVERS. The technical and organizational measures for the protection of personal data are part of information security management and must be continuously adapted to technical developments and organizational changes.

# Control of data protection

Compliance with the data protection policy and the applicable data protection laws is regularly reviewed through data protection audits and other checks. The Data Protection Officer and other authorized company units or commissioned external auditors are responsible for carrying out these checks. The results of the data protection checks must be reported to the Data Protection Officer. The SÜDVERS Management Board must be informed of the main results as part of the associated reporting obligations. Upon request, the results of the data protection checks shall be made available to the competent data protection authority. The competent data protection authority may carry out its own checks on compliance with the provisions of this policy, insofar as this is permitted under national law.

# Incidents in connection with data protection

All employees must inform their line manager or the Data Protection Officer immediately of any cases of breaches of this Data Protection Policy or other regulations on the protection of personal data (data protection incidents). The manager responsible for the function or business area is obliged to inform the data protection officer immediately of any data protection incidents.

In cases of

* unauthorized transfer of personal data to third parties,
* improper access by third parties to personal data, or
* Loss of personal data

the obliged legal entity must report the incident immediately so that any reporting obligations under national law can be fulfilled.