

Privacy policy relating to the use of the whistleblower system of the Südwestdeutsche Salzwerte AG

1. Our privacy policy

The protection of your personal data is a high priority at **Südwestdeutsche Salzwerte AG**. We therefore always treat your personal data, insofar as you provide it as part of your report via our whistleblower system, confidentially and in accordance with the applicable provisions on data protection.

This privacy policy is designed to inform you regarding the type, scope and purpose of the personal data we collect, use and process as part of our whistleblower system. This privacy policy also explains the rights of data subjects with respect to their personal data, **and what type of information (see sub-section 6 "What information can be reported through the whistleblower system?") may be submitted via this whistleblower system.**

2. Definitions of terms

Our privacy policy uses the same terms that are contained in the General Data Protection Regulation (hereinafter: "GDPR"). We have listed the most important terminology here to make it easier for you to read and understand this privacy policy.

2.1 Personal data

Personal data is any information relating to an identified or identifiable natural person (hereinafter the "data subject"). An identifiable natural person is an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of such natural person.

2.2 Data subject

A data subject is any identified or identifiable natural person whose personal data is processed by the controller.

2.3 Processing

Processing is any operation or set of operations which is carried out on personal data, whether by automated means, e.g. collection, recording, organisation, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.4 Restriction of processing

Restriction of processing is the marking of stored personal data with the aim of limiting their future processing.

2.5 Pseudonymisation

Pseudonymisation is the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

2.6 Data controller or entity responsible for processing

The data controller or entity responsible for processing is the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of the personal data. If the purposes and methods of such processing are determined by EU or Member State law, the controller or the specific criteria for its designation may be provided for under Union or Member State law.

2.7 Commissioned data processor

The processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2.8 Recipient

The recipient is a natural or legal person, public authority, agency or other body to whom personal data is disclosed, regardless of whether the recipient is a third party. However, authorities that may receive personal data in the context of a specific investigation mandate under Union or Member State law are not deemed recipients.

2.9 Third parties

A third party is a natural or legal person, public authority, agency or other body in addition to the data subject, the controller, the processor and the persons authorised to process the personal data under the direct responsibility of the controller or the processor.

2.10 Consent

Consent denotes any specific and informed indication of the data subject's wishes, granted voluntarily, in the form of a statement or other unambiguous

affirmative act whereby the data subject signifies their consent to the processing of their personal data.

3. Name and address of the controller / entity responsible for processing

The controller within the meaning of the GDPR, other data protection laws applicable in the Member States of the European Union and other provisions of a data protection nature is:

Südwestdeutsche Salzwerke AG

Salzgrund 67

74076 Heilbronn

Germany

4. Data Protection Officer contact details

You can contact the Data Protection Officer at the following address:

Südwestdeutsche Salzwerke AG

Data Protection Officer

Salzgrund 67

74076 Heilbronn

Alternatively, please use the following email address for your enquiries regarding data protection:

Datenschutz@salzwerke.de

5. IT-security and anonymity when using the whistleblower system

5.1 IT security

The whistleblower system is hosted by Schleupen SE ("Schleupen"), an independent party that ensures the security and anonymity of the system. Schleupen has taken the necessary technical and organisational measures to prevent personal data from being accidentally or unlawfully damaged or lost and to prevent unauthorised disclosure or misuse of the personal data. The processing of personal data is subject to strict controls and procedures and is carried out in accordance with accepted standard practices in this field.

All the data is transmitted and stored in encrypted form. No unencrypted information is sent over the open Internet.

5.2. Anonymity

The system does not log IP addresses and device IDs and does not use cookies. If a report is created on a computer on the network of the organisation, there is a risk that the web pages visited could be logged in the organisation's browsing history and/or log. This risk can be eliminated if a report is sent from a computer that is not connected to the organisation's own network. When uploading documents, you should be aware that the documents may contain metadata that could reveal your identity. Please therefore ensure that you remove all the identifying metadata from the document prior to uploading any material. You are free to decide if you make an anonymous report or one which contains personal data.

If a whistleblower chooses not to remain anonymous, their identity will become known to the persons handling the case.

In this case, the whistleblower may be called as a witness in a legal dispute and their identity may therefore be revealed.

Please note that if you provide any other information that directly or indirectly identifies you when you submit the report, the organisation will also process this information when handling the case.

This also applies if you submit the report anonymously.

6. What information can be reported through the whistleblower system?

You can use the whistleblower system to essentially report any breaches of compliance guidelines of Südwestdeutsche Salzwerte AG or violations of the law in particular according to the Whistleblower Protection Act. Compliance is understood as all the organisational measures implemented to observe the legal requirements and internal guidelines.

Accordingly, reports can be submitted in connection with the following topics:

- reports of legal violations under the Supply Chain Due Diligence Act
- reports of legal violations under the Whistleblower Protection Act
- Bribery and corruption
- Competition law
- Fraud, financial crime
- Food safety and quality
- Harassment or discrimination

- International trade controls
- Protection of personal data
- Rights and protection of persons, such as, but not limited to, violations of occupational health and safety regulations or general regulations serving the safety of employees
- Serious environmental damage or conflicts of interest

The following information and reports are not covered by the whistleblower system:

- References to issues including dissatisfaction with salary
- Difficulties in the working relationship between colleagues
- Violations of the smoking and alcohol These should be notified via the normal internal channels and reporting channels.

Notifications that are not handled via the whistleblower system will not be processed further. The term "organisation" refers to the company receiving the report.

7. What data is collected when using the whistleblower system and how is this data handled?

7.1 Log data for anonymous reporting

Reports entered into the whistleblower system are always anonymous, provided you choose to submit an anonymous report. In this case, only the report itself will be recorded. Neither the IP address nor the device ID of the computer on which the message was written are logged.

7.2 Personal data within the scope of the report

The system provides the following fields if you wish to enter your contact details:

- Name
- Telephone
- Email

If you submit personal data, **you should be aware** that the organisation may use your personal data as part of the investigation into the case and also in any subsequent legal proceedings.

The organisation guarantees that the right to protection of your personal data will be observed without restriction and that such information will only be used as described above.

The organisation does not share your personal data with third parties outside the organisation, except in the cases detailed in the following section.

7.3 Disclosure of information entered

Information entered into the whistleblower system is generally not shared with third parties outside the organisation. However, disclosure may occur in the following cases:

- Disclosure to an external legal representative in connection with the processing of the report
- If the report results in legal proceedings
- Due to statutory

7.4. Changes to the information entered

If you realise that you have provided incomplete or incorrect information, please immediately create a new report in the system, referring to your previous report and correct the information accordingly. You can make changes at any time by logging into the system with the report ID. If you have forgotten the report id, please create a new report and refer to the report you submitted previously.

7.5. Deletion of the data entered

The data entered will only be stored for as long as it is required. The information will be deleted if the storage of such is no longer necessary.

8. Principles of handling the case

We take all the notifications and reports of violations that are submitted via the whistleblower system seriously and will promptly initiate investigations into the case.

The investigation is led by the person responsible for the reporting procedure. The persons entrusted with the investigation will approach the matter objectively and will conduct discussions, examine the documentary evidence, establish the facts and will then contact staff who may have knowledge of the alleged incident. Please note that, during the investigations of the reports and notifications, further questions may be necessary that arise from such investigations. We will always send these queries to you within the whistleblowing system. Please therefore make a note of your report ID and check the whistleblower system regularly.

9. The legal basis for data processing in the whistleblower system

Processing is necessary for compliance with a legal obligation to which the organisation is subject. The organisation is legally obliged to set up and operate a whistleblower system.

Furthermore, data processing is necessary to safeguard the legitimate interests of the organisation when dealing with irregularities.

Processing is necessary to establish, exercise or defend legal claims or in the event of actions by the courts in the course of their judicial activities.

10. Your rights as a data subject at a glance

To the extent that you provide your personal data as part of your report entered via the whistleblower system and therefore do not remain anonymous, you as a data subject have rights of access in accordance with the provisions of the GDPR that can be asserted with respect to your personal data. Data subjects can therefore exercise their right of access, to rectification, erasure, to a restriction of processing, to data portability and individual rights to object to processing and a right to lodge a complaint with a supervisory authority. The following contains an overview of the individual rights and their deadlines.

10.1. Deadlines for rights of access in accordance with Art. 15 - 21 GDPR

As the controller, we will respond to any requests from the data subject pursuant to Art. 15 - 21 GDPR within one month after receipt. This deadline may be extended by an additional two months if this is necessary taking into account the complexity and number of applications. In this case, we will inform you within one month after receipt of your request regarding the extension. If the data subject makes the request electronically, we will respond to such electronically where possible, unless you indicate otherwise.

10.2 Channels for requests to exercise rights

Requests to exercise rights may be sent by surface post or email. The contact address is available under sub-section 4 of this privacy policy.

10.3 Right of access by the data subject pursuant to Art. 15 GDPR

A data subject has the right to obtain confirmation from the controller regarding whether their personal data is being processed and, if so, they have a right of access to such personal data and further information as described in Art. 15 GDPR.

Please note that the controller may only provide information if there are no doubts about the identity of the data subject. The controller will use all

reasonable means to verify the identity of a data subject who is seeking information.

10.4 Right to rectification pursuant to Art. 16 GDPR

A data subject shall have the right to obtain rectification from the controller of any inaccurate personal information without delay. Taking into account the purposes of the processing, the data subject has the right to request the completion of incomplete personal data, including via a supplementary statement.

10.5 Right to erasure pursuant to Art. 17 GDPR

A data subject has the right to require the controller to erase their personal data without undue delay and the controller shall erase personal data without undue delay if the conditions stipulated in Art. 17 GDPR are satisfied.

10.6 Right to restriction of processing pursuant to Art. 18 GDPR

The data subject has the right to request the controller to restrict processing if the conditions of Art. 18 GDPR are satisfied.

10.7 Right to data portability pursuant to Art. 20 GDPR

A data subject has the right to obtain the personal data concerning them which they have provided to a controller in a format stipulated in Art. 20 GDPR or to request such data to be transferred to another controller as instructed by the data subject, provided the conditions in Art. 20 GDPR are satisfied.

10.8 Right to withdraw consent pursuant to Art. 13 para 2 lit c GDPR

If the processing of the personal data of a data subject by the controller is pursuant to Art. 6 para 1 lit a GDPR [the data subject has consented to the processing of their personal data for one or more specific purposes] or Art. 9 para 2 lit a GDPR [The data subject has consented to the processing of special categories of their personal data for one or more specific purposes], the data subject has the right to withdraw their consent at any time without affecting the lawfulness of the processing carried out on the basis of consent up to the withdrawal of such.

You can request withdrawal by surface post or email. The contact address is available under sub-section 4 of this privacy policy.

11. Right to lodge a complaint with a supervisory authority pursuant to Art. 77 GDPR

Without prejudice to any other administrative or judicial remedy, data subjects reserve the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of their personal data infringes the GDPR. For this purpose, data subjects can generally contact the supervisory authority of their usual place of residence or workplace or the company head office.

The supervisory authority to which the complaint has been lodged shall inform the complainant of the status and outcome of such complaint and the potential judicial remedy in accordance with Art. 78 GDPR.

The competent data protection authority for us is:

The State Commissioner for Data Protection and Freedom of Information of Baden- Württemberg

Building address:

Lautenschlagerstraße 20

70173 Stuttgart

Germany

Postal address:

Postfach 10 29 32

70025 Stuttgart

Germany

For more information please visit: www.baden-wuerttemberg.datenschutz.de.

12. Topicality of this privacy policy

Amendments to our privacy policy may become necessary for legal or technical reasons. We reserve the right to make the relevant amendments at any time and therefore request that you consult this privacy policy at regular intervals to ensure you are aware of the current status of such.

Version: September 2023