

Data protection information

RWE ensures compliance with the law through a business model-oriented compliance organization, legally compliant processes and prevention and response measures. You can use the BKMS® system to report information by name or anonymously and securely to the responsible departments at RWE about (potential) misconduct damaging to the company or (potential) violations of laws, regulations or RWE internal rules or other risks or grievances affecting RWE that you have become aware of in the course of your work or in any other connection with RWE. These reports - hereinafter uniformly referred to as BKMS® reports - may include in particular (suspected) risks or violations of the following topics: RWE Code of Conduct, white-collar crimes (e.g. fraud, embezzlement, corruption), money laundering and terrorist financing, competition or antitrust law, data protection, information security, occupational safety or other security-related issues, discrimination and harassment in a professional context, tax law, other criminal or disorderly conduct and acts damaging to the company, as well as human rights and environmental risks and violations of human rights-related or environmental obligations as part of the complaints procedure under the Supply Chain Due Diligence Act (LkSG).

The protection of your personal data is important to us and you should always feel safe when using our whistleblowing system. You have the option of setting up a protected mailbox in the BKMS® system with a pseudonym/user name and password of your choice for further communication after submitting your BKMS® report. Against this background, we inform you in accordance with Art. 13 of the EU General Data Protection Regulation (GDPR) about the associated processing of your personal data via the [BKMS® system](#).

RWE will only process your data within the framework of the whistleblower system in accordance with the legally applicable provisions. These provisions result in particular from the GDPR and the Federal Data Protection Act (BDSG), the LkSG and provisions for the protection of whistleblowers (e.g. Whistleblower Protection Act - HinSchG). This data protection information contains explanations on data processing based on the whistleblower system.

1. Who is controller?

The RWE Group uses inter alia the central BKMS® system for reporting. The sole controller within the meaning of the EU General Data Protection Regulation ("GDPR") for this system is

RWE AG
Group Compliance
RWE Platz 6
45141 Essen

E-mail to compliance@rwe.com

If notifications are received that concern a company affiliated with RWE AG within the scope of Sections 15 et seq. AktG, RWE AG is jointly responsible with the RWE company concerned in the report for processing the incoming reports and the personal data contained in the reports.

In an agreement with the relevant RWE Group companies on joint responsibility in accordance with Article 26 GDPR, we have defined how the respective tasks and responsibilities for the processing of personal data are structured and who fulfils which data protection obligations. In this respect, RWE AG is responsible for the whistleblower system itself, the receipt and recording of whistleblowing reports and for the information obligations towards the data subjects (with the exception of the data subjects who are the subject of whistleblowing reports). The investigations to be carried out on the basis of reports are conducted and documented by RWE AG, if necessary with the involvement of the RWE Group company concerned, and, if necessary, follow-up measures are defined which are then implemented by the RWE Group company concerned under its sole responsibility. In addition, it was determined how an appropriate level of security can be ensured and how we can monitor potential data protection incidents. This also includes that the RWE Group company

Status: Jun 2024

concerned is responsible for fulfilling any reporting and notification obligations. You can also assert your rights in relation to processing under joint responsibility against another jointly responsible Group company. If you contact us, we will coordinate with the relevant Group companies in accordance with the agreement referred to in Article 26 GDPR in order to answer your request and guarantee your rights as a data subject.

2. How can you contact the data protection officer?

You can reach our data protection officer at

RWE AG
Data Protection Officer
RWE Platz 6
45141 Essen

[E-mail to datenschutz@rwe.com](mailto:datenschutz@rwe.com)

3. Which of your personal data do we process?

The use of the BKMS® system is voluntary. If you use the system, we may ask you to provide data relating to the following categories of data:

- Communication data (e.g. name, telephone, e-mail, address)
- Employee data of RWE employees and
- where applicable, names and contact details of individuals and other personal data (including special categories where the legal basis for this exists) of the individuals you name in your BKMS® notification.
- Storage of login data / use of cookies

To maintain the connection between your computer and the BKMS® system, a cookie is stored on your computer that only contains the session ID (so-called zero cookie). The cookie is only valid until the end of your session and becomes invalid when you close your browser.

4. What do we process your data for (purpose of processing) and on what legal basis?

The aim of the BKMS® system is to provide you with a communication channel for your BKMS® report and to ensure that it is processed properly.

In particular, we process your personal data for the following purposes:

- **Investigation of misconduct:** Information via the BKMS® system can serve to uncover and clarify in particular (internal/external) acts/omissions that are detrimental to the company, possible (labor) contractual breaches of duty or criminal offenses/regulatory violations as well as other grievances within the company.
- **Conflicts of interest:** Information about the BKMS® system also serves to uncover possible conflicts of interest that could facilitate the violation of laws or other breaches of regulations.
- **Prevention of future misconduct:** Furthermore, information via the BKMS® system can typically also prevent or at least impede future (internal/external) acts/omissions that are damaging to the company, breaches of (labor) contractual obligations or criminal offenses.
- **Exercise of rights:** Information via the BKMS® system can also serve to compensate for and defend against impending economic or other damages or disadvantages for RWE and thus for the effective legal

defense, exercise and enforcement of rights. For example, RWE may take measures to prepare (labor) court proceedings or other legal disputes on the basis of information provided.

- **Discharging employees:** RWE also takes appropriate measures to clarify possible allegations against employees of RWE who have been wrongly suspected and to discharge them.
- **Compliance with and implementation of legal obligations:** RWE is subject to comprehensive statutory supervisory and compliance obligations. These arise, among other things, from Sections 130 and 30 of the German Administrative Offenses Act (OWiG), Sections 93 and 111 of the German Stock Corporation Act (AktG) and from national regulations in countries in which RWE Group companies do business. In addition, reports via the BKMS® system can also be used to implement and comply with statutory data protection regulations, the provisions of the LkSG and the provisions for the protection of whistleblowers. Measures based on the whistleblower system typically serve to implement these legal obligations of RWE.

RWE will base permissible data processing within the framework of the whistleblower system on the following legal bases:

- **Consent (Art. 6 para. 1 lit. a):** Your information in the context of the whistleblower system is voluntary. In this context, information can also be provided anonymously.
- **Implementation of the employment relationship:** Data processing within the framework of the whistleblower system may be necessary, among other things, for the establishment, implementation and termination of the employment relationship with any employee concerned. Measures to uncover breaches of duty under the employment contract that do not constitute a criminal offense may also be justified. Measures may also be necessary for the handling of employment relationships, for example in the context of labor court disputes with the respective employee.
- **Investigation of criminal offenses:** If reports serve to uncover possible criminal offenses in the context of employment relationships, the corresponding data processing will only take place if documented factual indications justify the suspicion of a criminal offense in the employment relationship and the interests of the employee concerned do not prevail.
- **Implementation of legal obligations (Art. 6 para. 1 lit. c GDPR):** RWE is subject to comprehensive statutory supervisory and compliance obligations. The measures taken by RWE on the basis of notices also serve, among other things, to implement these legal obligations of RWE. In particular, the responsible reporting offices of RWE are authorized to process personal data, including special categories, in accordance with § 10 HinSchG, insofar as this is necessary to fulfill the obligations under the HinSchG.
- **Company agreements:** RWE may also process your data on the basis of applicable company agreements that specifically regulate the implementation of measures.
- **Protection of legitimate interests (Art. 6 para. 1 lit. f GDPR):** RWE may also process your data in order to protect their legitimate interests or those of a third party. These legitimate interests may include in individual cases:
 - **Legal defense:** Prevention of damage to the company. In this respect, data processing also serves the legitimate interests of RWE in the form of the assertion, defense and exercise of legal claims.

- **Improving compliance structures:** Information can also be used to improve RWE's internal compliance structures. For example, RWE can uncover and rectify possible weaknesses in its internal compliance organization on the basis of information provided. This is also a legitimate interest of RWE.
- **Support for persons named in BKMS® reports:** Information can also be used to discharge persons named in a BKMS® report. This is generally a legitimate interest of a third party.
- **Implementation of foreign legislation:** In addition to national and EU legal requirements, RWE is also subject to comprehensive legal provisions of countries outside the EU. The implementation of such foreign legislation is also generally recognized as a legitimate interest.

RWE will ensure that data collected as a result of reports will only be processed if the legitimate interests and rights of the data subjects do not outweigh this or if there is a legal obligation to process the data.

5. Disclosure of data and transfer to a third country

Your BKMS® report will be checked upon receipt and follow-up measures will be determined. Depending on the content of your report, the departments responsible for further processing at RWE will receive the information you have reported.

Apart from that, data contained in the BKMS® report may not be passed on without further ado. Statutory confidentiality requirements and any exceptions to the confidentiality requirement will be considered. If your consent is required for the disclosure of your data, we will obtain this in advance. Nevertheless, we would like to point out that we may be obliged to disclose your identity due to legal provisions or by official or court order.

Service providers (general)

RWE has assigned the company EQS Group AG, Karlstr. 47, 80333 München ("Service Provider") to operate the compliance reporting system on behalf of RWE and to store the data in a database operated by EQS Group AG in a high-security data center in the European Union.

RWE has also carefully selected the service provider and monitors it regularly, in particular its careful handling and protection of the data stored with it. All data is encrypted, password-protected and stored in a secure location so that access to the content of the electronically stored data is restricted to a narrow circle of authorized persons at RWE. As long as you yourself do not enter any data that allows conclusions to be drawn about your person, the whistleblower system automatically protects your anonymity by means of a certified procedure that is secured by comprehensive technical and organizational measures.

The service provider has been obligated by RWE to maintain confidentiality and to comply with legal requirements. The same requirements are observed if other (technical) service providers are involved in clarifying and processing the facts.

We may pass on the contents of the report and the results of the further clarification of the reported facts to courts, authorities and other public bodies. This may be the case if we are legally obliged to disclose the data or if this is necessary for the assertion, exercise or defense of legal claims.

In the course of clarification measures and in the assertion, exercise or defense of legal claims, we may also rely on the support of law firms or auditing companies.

Transfer to recipients outside the EU or EEA

Insofar as the legal requirements are met, we may also transfer personal data to RWE legal entities or authorities based outside the EU or the EEA in so-called third countries. In this case, we ensure before the transfer that the recipient either has an adequate level of data protection (e.g. due to an adequacy decision of the EU Commission for the respective country or the agreement of so-called EU standard data protection clauses with the recipient), that you have consented to the transfer or that the transfer is necessary for the assertion, exercise or defense of legal claims.

You can obtain an overview of the recipients in third countries and a copy of the agreed regulations to ensure an adequate level of data protection from us. Please use the contact details given in point 2 for this purpose.

6. How long do we store your data?

RWE will store or delete data collected as part of the whistleblower system and on the basis of subsequent measures in accordance with the relevant data protection regulations, in particular in accordance with Art. 17 GDPR in conjunction with Section 11 para. 5 HinSchG. § Section 11 (5) HinSchG. RWE will then delete the documentation three years after completion of the procedure. The documentation may be retained for longer in order to fulfill the requirements of the HinSchG or other legal provisions, as long as this is necessary and proportionate. The documentation of the fulfillment of the due diligence obligations under the LkSG must be kept for at least seven years from its creation.

7. What security measures do we have in place?

Incoming reports are processed exclusively by a narrow circle of expressly authorized and specially trained RWE employees. The employees entrusted with the processing of BKMS® reports and the service providers commissioned by us in this context are obliged to maintain confidentiality, secrecy and compliance with the applicable legal provisions (in particular data protection regulations, provisions for the protection of whistleblowers and provisions of the LkSG).

We take all necessary technical and organizational measures to ensure an appropriate level of protection and to protect your data managed by us, in particular against the risks of accidental or unlawful destruction, manipulation, loss, alteration or unauthorized disclosure or access. Our security measures are regularly improved in line with technological developments. Communication between your computer and the BKMS® system takes place via an encrypted connection (TLS).

8. What data protection rights do you have?

You can assert the following rights under the legal requirements:

- Art. 15 GDPR the right to information about the data processing and to receive a copy of the processed data,
 - Art. 16 GDPR the right to have incorrect data corrected,
 - Art. 17 GDPR, you have the right to have your data erased if there is no legal ground or no overriding legitimate grounds for further processing,
 - Art. 18 GDPR the right to demand restriction of processing,
 - In accordance with Art. 20 GDPR, you have the right to data portability with regard to all data that you have provided to us. This means that we will provide them to you in a structured, commonly used and machine-readable format and
- Art. 21 GDPR the right to object to data processing on the basis of Art. 6 para. 1 lit. f) GDPR, if this can be justified on the basis of your particular situation.

To exercise your rights, please use the contact details provided under point 2.

If you have given us separate consent to process your personal data, you can withdraw this consent at any time. The legality of the processing of your data up to the time of revocation remains unaffected by a revocation.

Without prejudice to any other administrative or judicial remedy, you have the right to complain to a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of personal data relating to you infringes relevant data protection regulations.

An overview of the data protection supervisory authorities with their contact information is available on the website of the [Federal Commissioner for Data Protection and Freedom of Information](#).

9. Automated decision-making including profiling

Automated decision-making, including profiling, does not take place within the framework of the whistleblower system.

10. Is there an obligation to provide your personal data?

The provision of your personal data via the BKMS® system is neither legally nor contractually required.