

Information on Data Protection in Accordance with Art. 13 and Art. 14 GDPR (EU General Data Protection Regulation)

KIT Whistleblower System

The following information provides you with an overview of the processing of your personal data in connection with whistleblowing and your rights under data protection law. According to Art. 4, No. 1 of the EU General Data Protection Regulation (GDPR), personal data is any information referring to an identified or identifiable natural person.

Contents

| | |
|---|---|
| 1. Responsible Person and Data Protection Commissioner | 1 |
| 2. Accessing the Website https://hinweis.comp.kit.edu/ and Server Log Files | 2 |
| 3. Data Processing when Using the Whistleblower System..... | 2 |
| a. Registration and Login to the Electronic Whistleblower Portal at https://hinweis.comp.kit.edu/ | 3 |
| b. Personal Data in the Course of Whistleblowing | 3 |
| c. Forwarding of Personal Data | 4 |
| 4. Cookies on the Website https://hinweis.comp.kit.edu/ | 4 |
| 5. Encryption and Data Security | 5 |
| 6. Your Rights | 5 |

Content Details

1. Responsible Person and Data Protection Commissioner

The controller for data processing within the meaning of the GDPR (Art. 4, No. 7) and other data protection regulations is:

Karlsruhe Institute of Technology (KIT)

Kaiserstraße 12

76131 Karlsruhe

Germany

Phone: +49 721 608-0

Fax: +49 721 608-44290

Email: info@kit.edu

The Karlsruhe Institute of Technology is a corporation under public law. It is represented by the respective president.

Our **Data Protection Commissioner** can be contacted at dsb@kit.edu or by ordinary mail with “Die Datenschutzbeauftragte” (the data protection commissioner) being indicated on the envelope.

2. Accessing the Website <https://hinweis.comp.kit.edu/> and Server Log Files

Scope and purpose: When using the website for information purposes only, i.e. when you do not register or transmit other information, we will only collect the personal data that are transmitted by your browser to our server according to the settings made by you (server log files) for the purpose of enabling you to access the website.

- Anonymized IP address
- Date and time of access
- Time zone difference to Greenwich Mean Time (GMT)
- Content of the access (concrete site)
- Status of access/HTTP status code
- Data volume transmitted
- Website from which an accessing system reaches our website
- Browser

The data is used for the technical optimization of the website and to ensure the security of our information technology systems. The IP address is necessary for the operation and delivery of the website, is shortened in the log files and is no longer available as a whole after the request. It is not possible for us to draw direct conclusions about individual persons from this data. A comparison with other databases does not take place.

Recipients: The data will not be passed on to third parties.

Legal basis: The legal basis for the temporary processing of data is Art. 6, par. 1 (f) GDPR. Since the processing of this data is absolutely necessary, there is no possibility of objection. The above-mentioned purposes also constitute KIT's legitimate interest in data processing in accordance with Art. 6, par. 1 (f) GDPR.

Storage period: The above-mentioned data is only processed so that the website can be accessed. The data will not be stored.

3. Data Processing when Using the Whistleblower System

The KIT whistleblower system offers the opportunity to report compliance violations via various communication channels in person, by telephone or in writing, stating your own contact details or anonymously. The purpose of this reporting option is to identify legal and/or regulatory violations (such as criminal offenses, administrative offenses or violations of internal regulations) at KIT or at KIT suppliers, to initiate internal investigations and to take measures to ensure compliance with laws and regulations. Through its whistleblower system, KIT also implements the obligation to set up an internal reporting office in accordance with Article 12 par. 1, Article 14 par. 1 of the German Whistleblower Protection Act (Hinweisgeberschutzgesetz - HinSchG), as well as the obligation to set up a complaints procedure in accordance with Article 8 of the German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz - LkSG). In addition to direct contact with the Compliance Staff Unit (in person, by telephone or in writing by post or email), the KIT's electronic whistleblower portal at <https://hinweis.comp.kit.edu/> is available for submitting information anonymously.

a. Registration and Login to the Electronic Whistleblower Portal at <https://hinweis.comp.kit.edu/>

Scope and purpose: To use the electronic whistleblower portal of the KIT as a whistleblower or to log in for the purpose of using it, registration is required. To do this, you can enter a user name and password of your choice. You can choose the user name freely, i.e. you can decide for yourself whether it is personal or anonymous. After your registration, you can log in to the portal via the start page of the website.

Recipients: Only the authorized employees of the Compliance Staff Unit (COMP) have access to the registration/login data.

Legal basis: The legal basis for the processing is Art. 6, par. 1 (c), par. 3 GDPR and Art. 9, par. 2 (g) GDPR in conjunction with Art. 10, 12 Whistleblower Protection Act.

Storage period: If you have provided personal data during registration, this data will be stored for as long as is necessary for the above-mentioned purposes, i.e. until the compliance case has been resolved and closed. As soon as a case has been rejected or closed by COMP, it will be blocked in the whistleblower portal by COMP. After 4 weeks following the blocking of the case, the entire process and the registered account are automatically deleted from the portal database.

b. Personal Data in the Course of Whistleblowing

Data source, scope and purpose: Personal data from a submitted information, such as communication data (e.g. name, telephone, email, address), employee data of KIT employees (e.g. KIT account, OU affiliation), as well as other personal data mentioned, are processed for investigation. This may be data of the person providing the information, of affected persons, contributors, witnesses or other persons associated with the facts of the case.

Recipients: Only the authorized employees of the Compliance Staff Unit (COMP) have access to the data.

Legal basis: The legal basis for the processing is Art. 6, par. 1 (c), par. 3 GDPR and Art. 9, par. 2 (g) GDPR in conjunction with Art. 10, 12 Whistleblower Protection Act.

Storage period: Personal data is stored for as long as is necessary for the clarification and final processing of the compliance case. This also includes any resulting internal measures to rectify deficiencies or for prevention, any resulting legal or administrative proceedings and any other assertion of rights in connection with the case.

As soon as a case has been rejected or closed by COMP, it will be blocked in the whistleblower portal. After 4 weeks following the blocking of the case, the entire process and the registered account are automatically deleted from the portal database.

In addition, COMP creates an electronic file for each case in the internally used file management system, in which the submitted information and its further processing are documented. The data from the whistleblower portal is stored as a PDF export in the electronic file for documentation purposes. The documentation of the submitted information will be deleted three years after completion of the procedure in accordance with Art. 11, par. 5 of the Whistleblower Protection Act. It may be stored for longer in order to meet the requirements of the Whistleblower Protection Act or other legal provisions, as long as this is necessary and proportionate.

c. Forwarding of Personal Data

Scope and purpose, recipients: Personal data of the whistleblower will only be passed on to other persons or bodies responsible for further processing/investigation and for follow-up measures if the whistleblower has previously consented to the transfer and this is necessary to the examination of the case. Statutory or official notification obligations are excluded from this.

Personal data of other persons named in the information may, if necessary, be passed on to other persons or bodies responsible for further processing/investigation and for follow-up measures. In addition, it may be necessary to pass on personal data to other persons to clarify the facts (e.g. in the context of witness interviews or when obtaining information from the central administration of the KIT). Furthermore, it may be necessary to pass on data to other responsible parties (e.g. authorities, due to legal provisions or by enforceable official or court order, or for the purpose of reporting criminal offenses).

Legal basis: Processing by the internal reporting office as necessary to fulfill its tasks is based on Art. 6, par. 1 (c) GDPR in conjunction with Articles 10 and 12 of the Whistleblower Protection Act. Processing for other purposes (forwarding to the competent bodies within the employer; e.g. in order to carry out further investigations or take steps under labor law in the event of substantiated information) is based on Art. 6, par. 1 (c) GDPR and Articles 10, 12, 13, 18, No. 4 (a) and 9, par. 3 and 4, No. 2 of the Whistleblower Protection Act.

The forwarding of the identity of the whistleblower or other circumstances that allow conclusions to be drawn about the identity of this person is based on Art. 6, par. 1 (a) GDPR (consent). Consent is voluntary. If it is refused or revoked, there are no disadvantages. Consent can be revoked by sending a message to info@comp.kit.edu.

Storage period: The further processing of data (e.g. investigative measures, follow-up measures) is not subject to the time limits of the Whistleblower Protection Act. The respective responsible bodies store the data for as long as this is necessary for the purposes pursued.

4. Cookies on the Website <https://hinweis.comp.kit.edu/>

Scope and purpose: We use so-called session cookies (transient cookies), which are technically necessary to make the website functional. The language setting data is stored and transmitted in the cookies we use.

Recipients: The data will not be passed on to third parties.

Storage period: The session cookies are deleted at the latest when you close the browser.

Tip: You can set your browser such that you are informed about the setting of cookies and you can permit cookies in individual cases only, exclude the acceptance of cookies for certain cases or in general and activate automatic deletion of cookies when closing the browser. When deactivating cookies, functionality of this website may be limited.

5. Encryption and Data Security

For reasons of security and for the protection of the transmission of confidential contents, such as inquiries sent to us as website operator, this website uses TLS encryption. In case of an encrypted connection, the address line of the browser changes from http:// to https:// and the lock symbol is indicated in your browser line. When TLS encryption is activated, third parties cannot read the data you transmit to us as a rule. Please note, however, that when data is transmitted over the Internet, it is never possible to guarantee complete protection against access by third parties.

In addition, the following measures are implemented in the electronic whistleblower portal:

- Upon registration or log-in, an own 1024-bit key pair is generated for the account by OpenSSL. The private key is protected by the selected password.
- All messages are stored in the database, one version coded with the public key of the whistleblower and one version with the public key of the Compliance Commissioner or the staff of COMP.
- When a process is blocked, all corresponding entries in the database, the account, and the generated key pair are deleted.

6. Your Rights

As far as your personal data are concerned, you have the following rights:

- Right to revoke your consent with effect for the future, provided that the processing is based on consent pursuant to Art. 6, par. 1, subpar. 1 (a) GDPR (Art. 7, par. 3 GDPR)
- Right to confirmation as to whether data concerning you is being processed and to information about the processed data, to further information about the data processing and to copies of the data (Art. 15 GDPR)
- Right to rectification or completion of inaccurate or incomplete data (Art. 16 GDPR)
- Right to immediate erasure of data concerning you (Art. 17 GDPR)
- Right to restriction of processing (Art. 18 GDPR)
- Right to receive the data in a structured, commonly used and machine-readable format, provided that the processing is based on consent pursuant to Art. 6, par. 1, subpar. 1 (a) or Art. 9, par. 2 (a) GDPR or on a contract pursuant to Art. 6, par. 1, subpar. 1 (b) GDPR (Art. 20 GDPR)
- Right to object to the future processing of data concerning you, provided that the data are processed in accordance with Art. 6, par. 1 (e) or (f) GDPR (Art. 21 GDPR)

Furthermore, you have the right to complain to the supervisory authority about the processing of your personal data by KIT (Art. 77 GDPR). The supervisory authority for KIT within the meaning of Art. 51, par. 1 GDPR is in accordance with Art. 25, par. 1 State Data Protection Act Baden-Wuerttemberg (Landesdatenschutzgesetz - LDSG):

The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (<https://www.baden-wuerttemberg.datenschutz.de/>).