Technology
Arts Sciences
TH Köln

Reporting Office under the Whistleblower Protection Act

English version of the website for the reporting office in accordance with the Whistleblower Protection Act.

Version: 15. Juli 2025

Technology
Arts Sciences
TH Köln

Table of Contents

Technology
Arts Sciences
TH Köln

Whistleblower Protection Act (HinSchG)

Technische Hochschule Köln (TH Köln)

Your Report Matters — We Protect You.

Do you have knowledge of legal violations or misconduct at TH Köln? Would you like to report such an incident and remain anonymous? Then please contact TH Köln's Whistleblower Reporting Office. Here, you can submit your information securely and confidentially. All data is transmitted in encrypted form to ensure your identity remains protected. Every report is reviewed thoroughly and responsibly, and appropriate measures will be taken to clarify and stop the violation.

TH Köln thereby complies with the requirements of the German Whistleblower Protection Act (HinSchG).

Version: 15. Juli 2025

Technology
Arts Sciences
TH Köln

Frequently Asked Questions (FAQs)

Why Should I Submit a Report?

Your reports help us uncover legal violations and uphold the integrity of TH Köln. Misconduct harms the credibility of our university.

What Types of Reports Are Processed?

You can report violations of laws (e.g., criminal offenses or administrative violations) that you become aware of in the context of your professional activities. For more details, please refer to Section 2 of the Whistleblower Protection Act.

The reporting office is available to all employees, suppliers, service providers, and other individuals professionally associated with TH Köln.

For breaches of internal university policies such as discrimination or bullying, please contact the respective responsible office within TH Köln.

How Do I Submit a Report?

Reports can be submitted using any internet-enabled device by clicking the “Submit Report” button.

The reporting process involves four steps:

1. Read the information on protecting your anonymity and complete a security query.
2. Indicate the main focus of your report.
3. Choose whether to report anonymously or under your name. Describe the issue in your own words and answer follow-up questions using a simple selection format. You have up to 5,000 characters for free text and may upload one file (max. 5 MB). Please be aware that files may contain metadata identifying the author. After submitting your report, you will receive a reference number as confirmation.

4. Set up your secure personal mailbox. This mailbox will be used for follow-up questions and status updates — you will remain anonymous throughout the process.

If you already have a mailbox, you can access it via the “Login” button. A security query will also be required there.

Your anonymity is technically protected as long as you do not enter any identifying information yourself.

How Do I Receive Feedback While Remaining Anonymous?

By setting up a secure mailbox, you will receive updates and — if necessary — follow-up questions regarding your report. Communication through this mailbox remains fully anonymous.

You choose your own pseudonym/username and password. These credentials are not visible to anyone else. If you lose your login details, you will need to submit a new report and set up a new mailbox — please reference your previous report number if possible. Note that your previous messages will not be visible in the new mailbox.

Anonymity is certified by an independent third party. Your report is kept anonymous through encryption and special security measures.

To preserve anonymity:

- Do not include identifying information in your report.
- Avoid using devices (PC or smartphone) belonging to your employer.

What Happens After I Submit a Report?

If you set up a mailbox, you will promptly receive a confirmation of receipt. The reporting office will review your report and may contact you for additional information.

Within three months, you will receive feedback via the secure mailbox on the status and any actions taken — unless doing so would jeopardize the investigation or the rights of the individuals named in the report.

If your report falls outside the scope of the Whistleblower Protection Act, you will be informed and, with your consent, your report may be forwarded to the appropriate authority.

About the Whistleblower Reporting Office

The function of the Whistleblower Reporting Office at TH Köln is assigned to the Internal Audit Department, which holds the necessary authority and responsibilities in accordance with Section 15 of the Whistleblower Protection Act.

The appointed officer of the reporting office performs duties under Section 13(1) HinSchG, including:

- Operating reporting channels (§ 16 HinSchG)
- Managing the reporting procedure (§ 17 HinSchG)
- Taking follow-up measures (§ 18 HinSchG)

The appointed officer acts independently in the exercise of these duties.

What Should I Consider Before Submitting a Report?

It is important that, at the time of submission, you have reasonable grounds to believe that the information you are reporting is accurate. Please clearly indicate if your report is based on a well-founded suspicion or information from third parties rather than verifiable facts.

Deliberate or grossly negligent submission of false information may constitute an administrative offense under the HinSchG and may also fall under Section 164 of the German Criminal Code (StGB).

What Alternatives Are Available?

You are free to submit your report alternatively or additionally to an **external reporting office**. These are subject to the same protective regulations as TH Köln's internal office.

External reporting offices include:

- Federal Office of Justice:
  https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes_node.html
- Federal Cartel Office (Bundeskartellamt):
  https://www.bkms-system.net/bkwebanon/report/channels?id=bkarta&language=ger
- Federal Financial Supervisory Authority (BaFin):
  https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html

More information on the responsibilities of each office:
https://www.bundesjustizamt.de/DE/MeldestelledesBundes/ZustaendigkeitderMeldestellen/ZustaendigkeitderMeldestellen_node.html

Criminal offenses can also be reported directly to the **police or public prosecutor's office**.

Rights of the Person Named in the Report

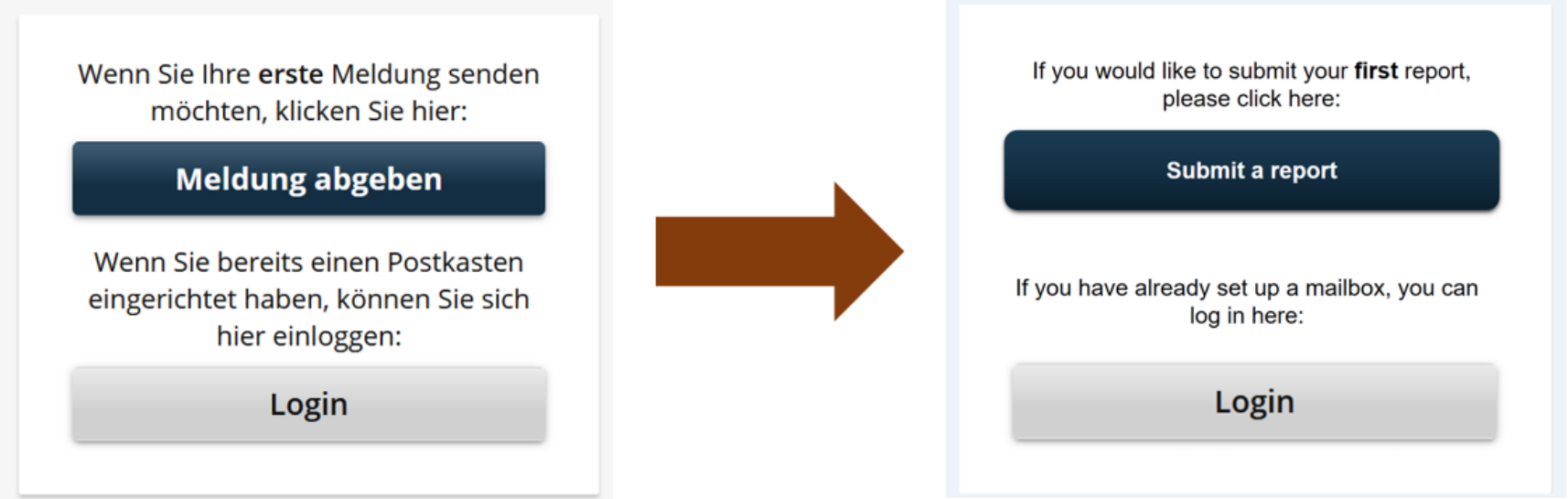
The identity of the person named in the report must also be protected. However, it may be disclosed by the reporting office if necessary for internal investigations or follow-up actions, or to authorities in the context of criminal or administrative proceedings.

If a report is intentionally or grossly negligently false and causes harm to the person affected, they are entitled to claim damage,

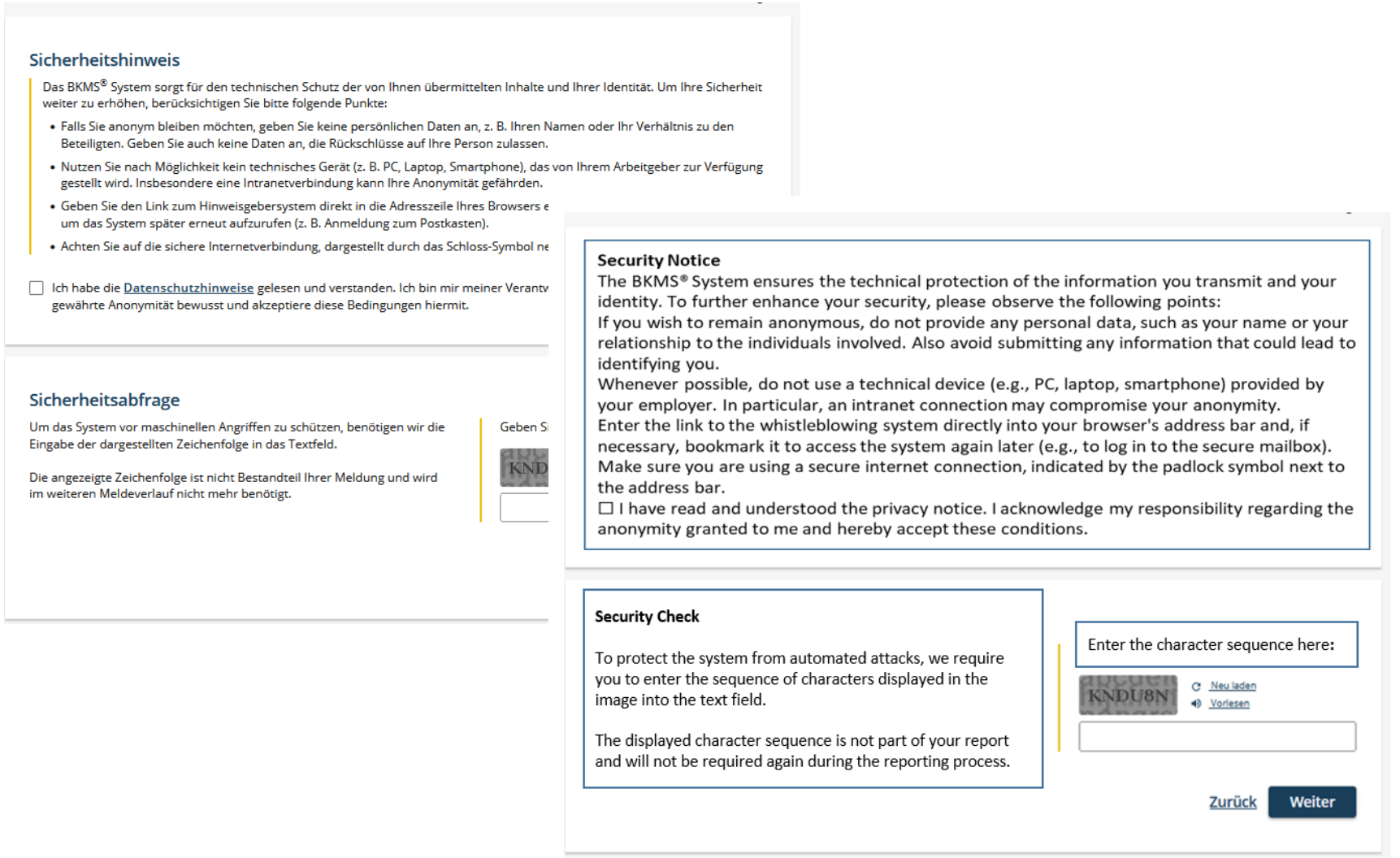
Technology
Arts Sciences
TH Köln

How do I submit a report?

1) **To submit a report, you need to click the blue button “Submit a report/Meldung abgeben”**



2) In the next step, you must confirm the privacy policy. Please find the translated privacy policy attached.



Sicherheitshinweis

Das BKMS® System sorgt für den technischen Schutz der von Ihnen übermittelten Inhalte und Ihrer Identität. Um Ihre Sicherheit weiter zu erhöhen, berücksichtigen Sie bitte folgende Punkte:

- Falls Sie anonym bleiben möchten, geben Sie keine persönlichen Daten an, z. B. Ihren Namen oder Ihr Verhältnis zu den Beteiligten. Geben Sie auch keine Daten an, die Rückschlüsse auf Ihre Person zulassen.
- Nutzen Sie nach Möglichkeit kein technisches Gerät (z. B. PC, Laptop, Smartphone), das von Ihrem Arbeitgeber zur Verfügung gestellt wird. Insbesondere eine Intranetverbindung kann Ihre Anonymität gefährden.
- Geben Sie den Link zum Hinweisgebersystem direkt in die Adresszeile Ihres Browsers e
um das System später erneut aufzurufen (z. B. Anmeldung zum Postkasten).
- Achten Sie auf die sichere Internetverbindung, dargestellt durch das Schloss-Symbol ne

☐ Ich habe die Datenschutzhinweise gelesen und verstanden. Ich bin mir meiner Verantv
gewährte Anonymität bewusst und akzeptiere diese Bedingungen hiermit.

Sicherheitsabfrage

Um das System vor maschinellen Angriffen zu schützen, benötigen wir die Eingabe der dargestellten Zeichenfolge in das Textfeld.

Die angezeigte Zeichenfolge ist nicht Bestandteil Ihrer Meldung und wird im weiteren Meldeverlauf nicht mehr benötigt.

Geben Si

KND

Security Notice

The BKMS® System ensures the technical protection of the information you transmit and your identity. To further enhance your security, please observe the following points:
If you wish to remain anonymous, do not provide any personal data, such as your name or your relationship to the individuals involved. Also avoid submitting any information that could lead to identifying you.
Whenever possible, do not use a technical device (e.g., PC, laptop, smartphone) provided by your employer. In particular, an intranet connection may compromise your anonymity.
Enter the link to the whistleblowing system directly into your browser's address bar and, if necessary, bookmark it to access the system again later (e.g., to log in to the secure mailbox).
Make sure you are using a secure internet connection, indicated by the padlock symbol next to the address bar.
☐ I have read and understood the privacy notice. I acknowledge my responsibility regarding the anonymity granted to me and hereby accept these conditions.

Security Check

To protect the system from automated attacks, we require you to enter the sequence of characters displayed in the image into the text field.

The displayed character sequence is not part of your report and will not be required again during the reporting process.

Enter the character sequence here:

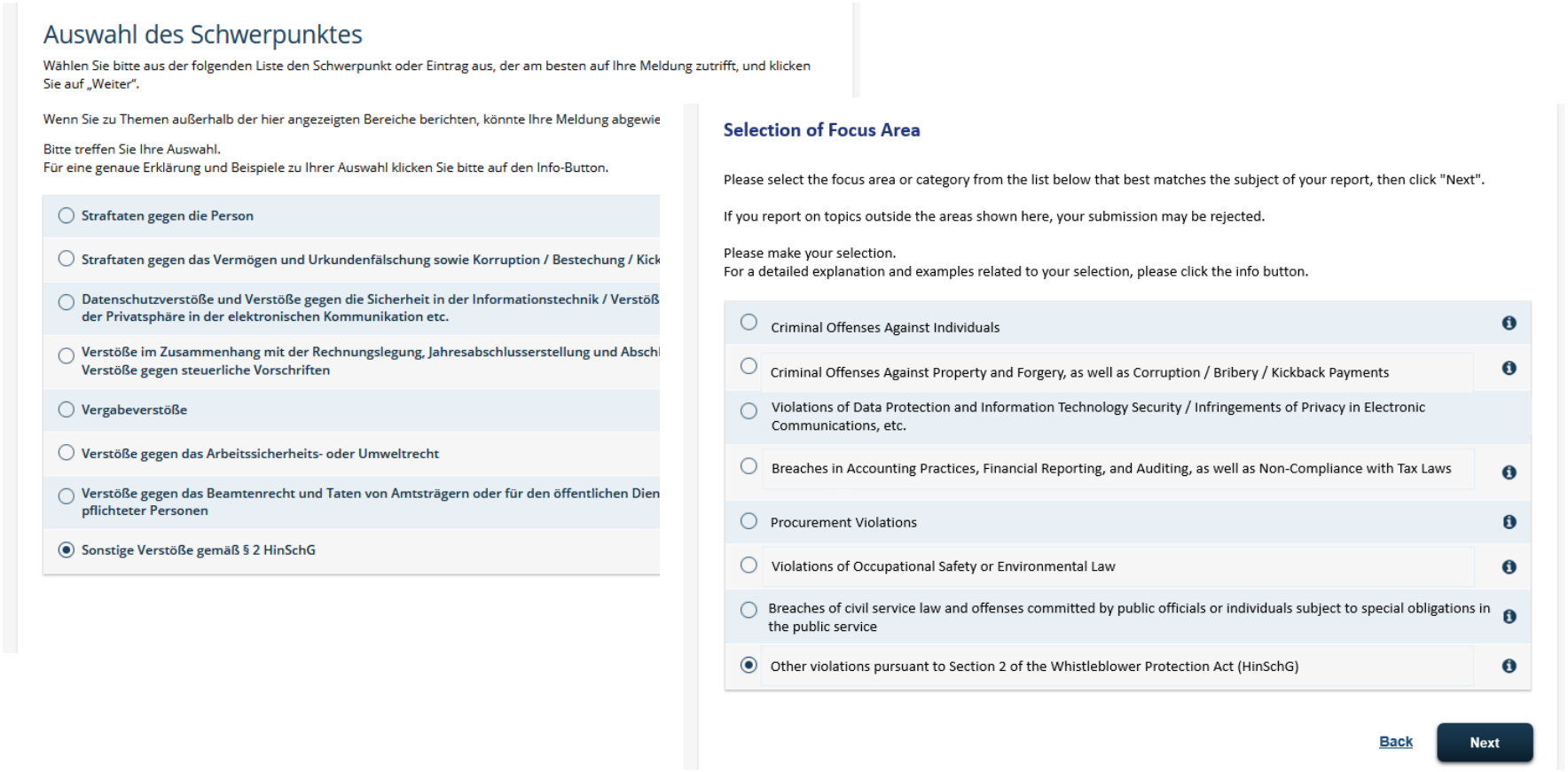
KNDU8N

Neu laden
Vorlesen

Zurück

Weiter

3) Once you have accepted the privacy policy and entered the character sequence, the individual topic categories will be displayed.



The following section provides a detailed explanation of the aforementioned key areas:

Criminal Offenses Against Individuals

This category also includes offenses against personal freedom, honor, and the right to privacy and confidentiality.

Examples of criminal offenses covered by this category include:

- Offenses against sexual self-determination
- Offenses causing bodily harm
- Unlawful deprivation of liberty
- Violation of the confidentiality of spoken words through unauthorized audio recordings
- Insult or defamation

If you have knowledge of serious criminal offenses that have occurred or are imminent, we strongly advise you to contact the police and public prosecutor's office directly.

Criminal Offenses Against Property and Forgery, as well as Corruption / Bribery / Kickback Payments

Criminal offenses against property include all acts related to the unlawful appropriation or damage of assets or possessions. This category comprises, for example, the following offenses:

- Theft
- Embezzlement
- Property damage
- Robbery
- Fare evasion or obtaining services by deception
- Fraud (including subsidy fraud)
- Breach of trust
- Misuse of checks and credit cards

Forgery of documents may be deemed to have occurred in connection with actions such as:

- Manipulating documents or financial statements
- Retrospectively altering delivery notes or invoices
- Creating fictitious invoices
- Forging certificates or academic transcripts (e.g., employment references, university diplomas, grade reports, etc.)

Corruption refers to the offering or solicitation of improper advantages in exchange for the performance of certain actions, such as preferential treatment in competitive processes or the exercise of official duties.
This typically—but not exclusively—includes violations of criminal provisions such as Sections 299 and 331 et seq. of the German Criminal Code

(StGB), as well as the bribery of elected officials (Section 108e StGB) or members of works councils and staff councils (Section 119 of the Works Constitution Act – BetrVG).

Violations of Data Protection and Information Technology Security / Infringements of Privacy in Electronic Communications, etc.

Data protection violations (i.e., breaches of data protection laws and regulations governing the safeguarding of personal data) include, in particular:

- The unlawful disclosure of trade and business secrets
- The misuse or unauthorized disclosure of personal data
- Inadequate access protection for sensitive data

Violations of IT security include, for example, the following actions:

- Unauthorized access to email accounts or IT systems
- Breach of telecommunications confidentiality

Breaches in Accounting Practices, Financial Reporting, and Auditing, as well as Non-Compliance with Tax Laws

This includes, for example, the following actions:

- Violations of commercial and tax record-keeping and retention requirements
- Tax crimes and regulatory tax offenses

Procurement Violations

This refers to violations of federal provisions and uniformly applicable regulations for contracting authorities concerning the procedures for the award of public contracts and concessions (including legal remedies in such procedures), once the relevant EU thresholds have been reached.

Violations of Occupational Safety or Environmental Law

This subject area includes, for example:

- Violations of occupational health and safety regulations, working time provisions, or regulations concerning rest periods and similar requirements
- Illegal waste disposal, improper handling of hazardous substances, as well as pollution of water, soil, or air

Breaches of civil service law and offenses committed by public officials or individuals subject to special obligations in the public service

The Whistleblower Protection Act (HinSchG) explicitly mentions statements made by civil servants that constitute a breach of their duty to uphold the constitutional order.

Also relevant are, for example:

- Criminal offenses committed in public office, such as accepting benefits, bribery, granting of advantages, and corruption (Sections 331 et seq. of the German Criminal Code – StGB)

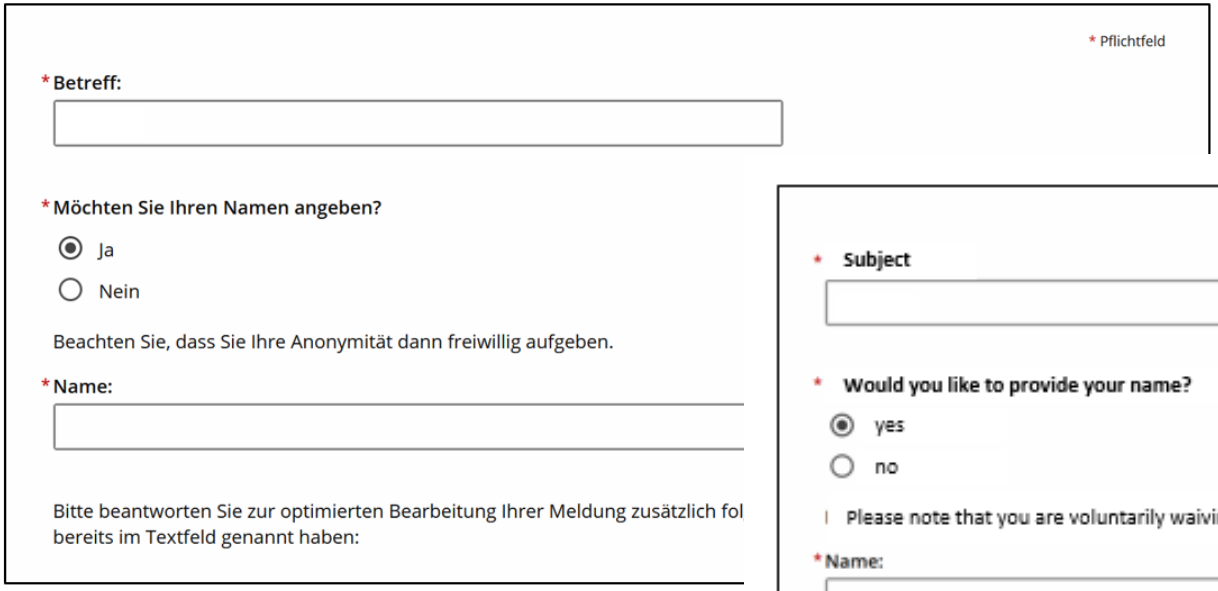
Other violations pursuant to Section 2 of the Whistleblower Protection Act (HinSchG)

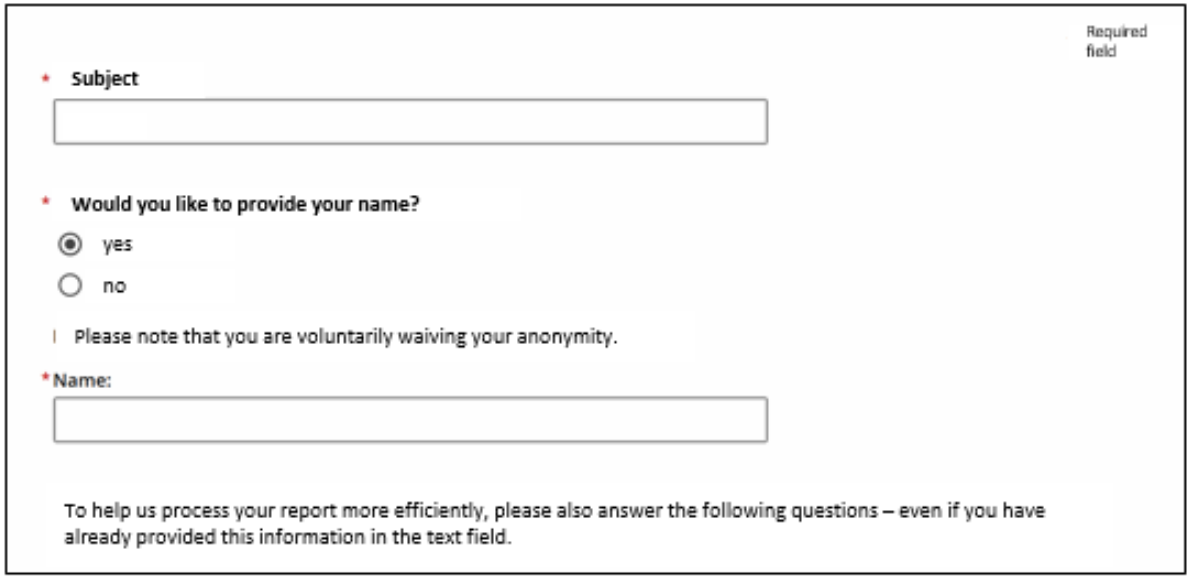
If your report does not fall under any of the aforementioned categories, it may concern another type of violation pursuant to Section 2 of the Whistleblower Protection Act (HinSchG). Such violations may also be reported here.

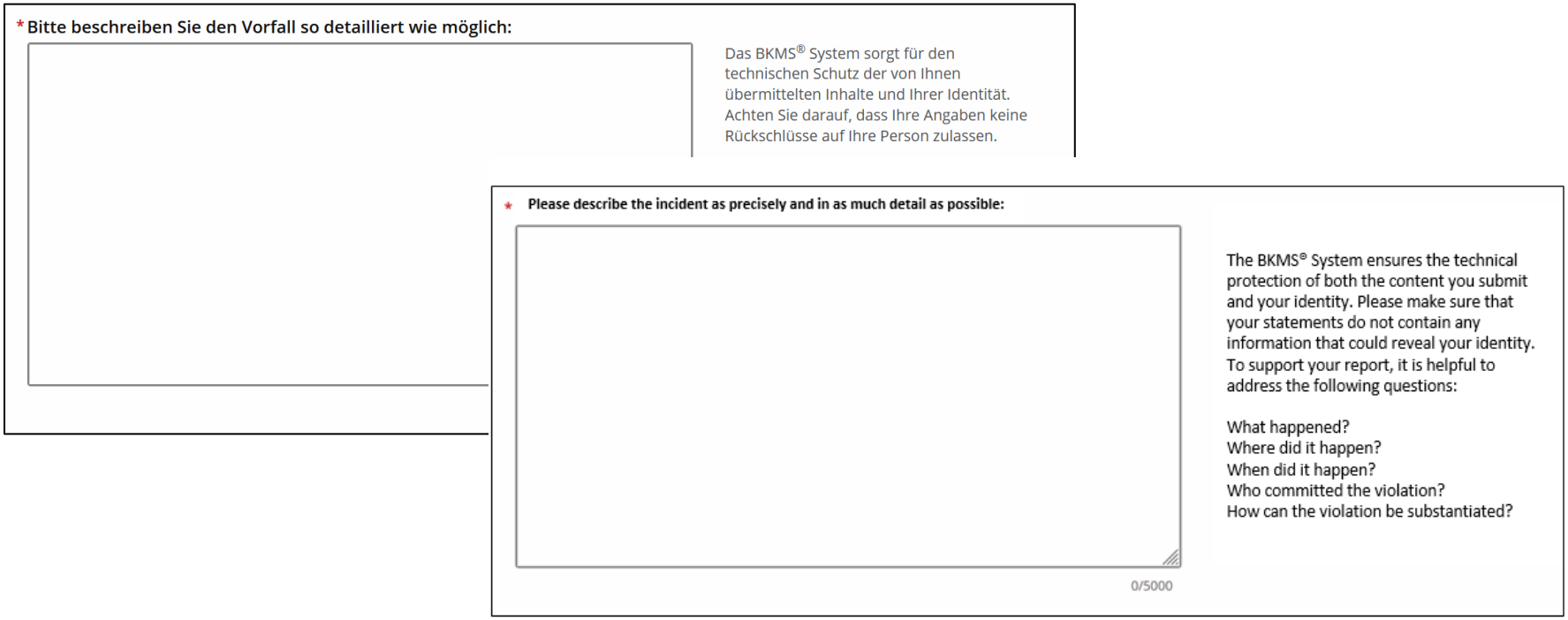
If your concern falls under multiple of the categories listed above, you may still submit the report through this channel.

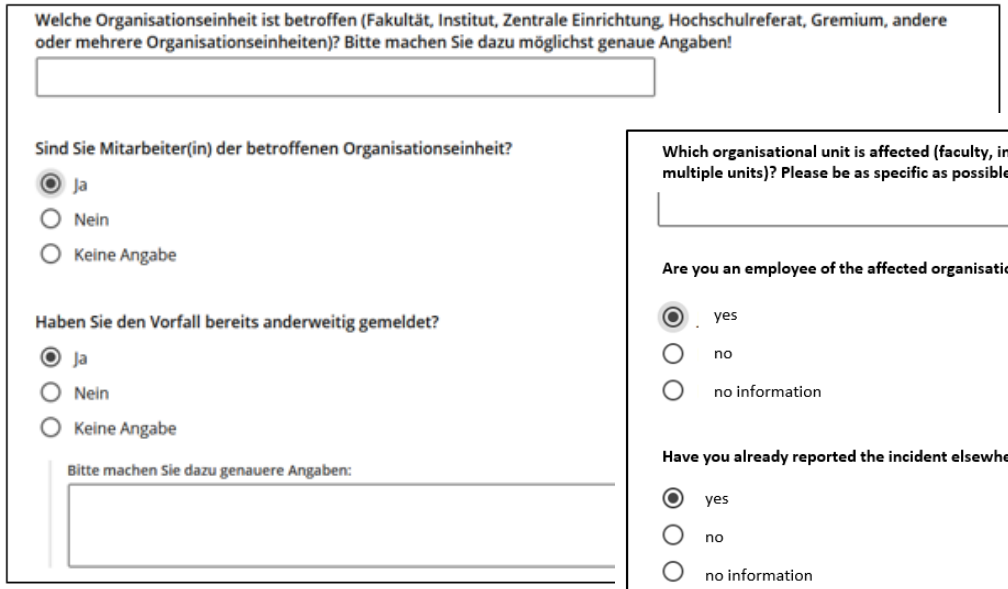
If the violation you report does not fall within the personal or material scope of the HinSchG, we will inform you accordingly and, with your consent, forward the report to the competent authorities.

4) After you have selected the relevant category, the input form for the actual report will open. Here, you can enter all necessary details and, if applicable, upload relevant documents.






* Bitte beschreiben Sie den Vorfall so detailliert wie möglich:
Das BKMS® System sorgt für den technischen Schutz der von Ihnen übermittelten Inhalte und Ihrer Identität. Achten Sie darauf, dass Ihre Angaben keine Rückschlüsse auf Ihre Person zulassen.
* Please describe the incident as precisely and in as much detail as possible:
0/5000
The BKMS® System ensures the technical protection of both the content you submit and your identity. Please make sure that your statements do not contain any information that could reveal your identity. To support your report, it is helpful to address the following questions:
What happened?
Where did it happen?
When did it happen?
Who committed the violation?
How can the violation be substantiated?


Welche Organisationseinheit ist betroffen (Fakultät, Institut, Zentrale Einrichtung, Hochschulreferat, Gremium, andere oder mehrere Organisationseinheiten)? Bitte machen Sie dazu möglichst genaue Angaben!

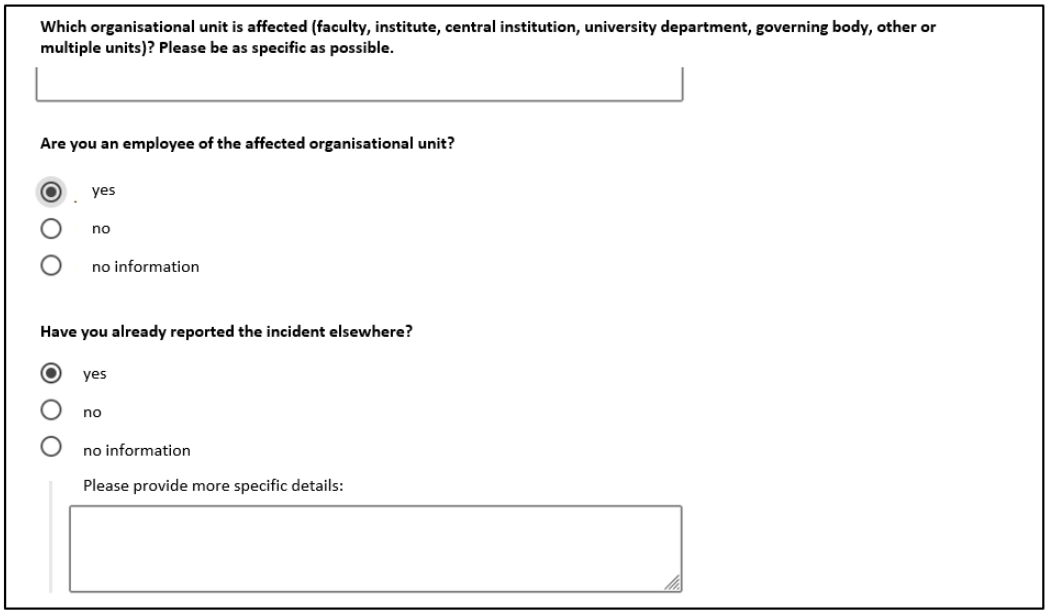
Sind Sie Mitarbeiter(in) der betroffenen Organisationseinheit?

- (•) Ja
- ( ) Nein
- ( ) Keine Angabe

Haben Sie den Vorfall bereits anderweitig gemeldet?

- (•) Ja
- ( ) Nein
- ( ) Keine Angabe

Bitte machen Sie dazu genauere Angaben:


Which organisational unit is affected (faculty, institute, central institution, university department, governing body, other or multiple units)? Please be as specific as possible.

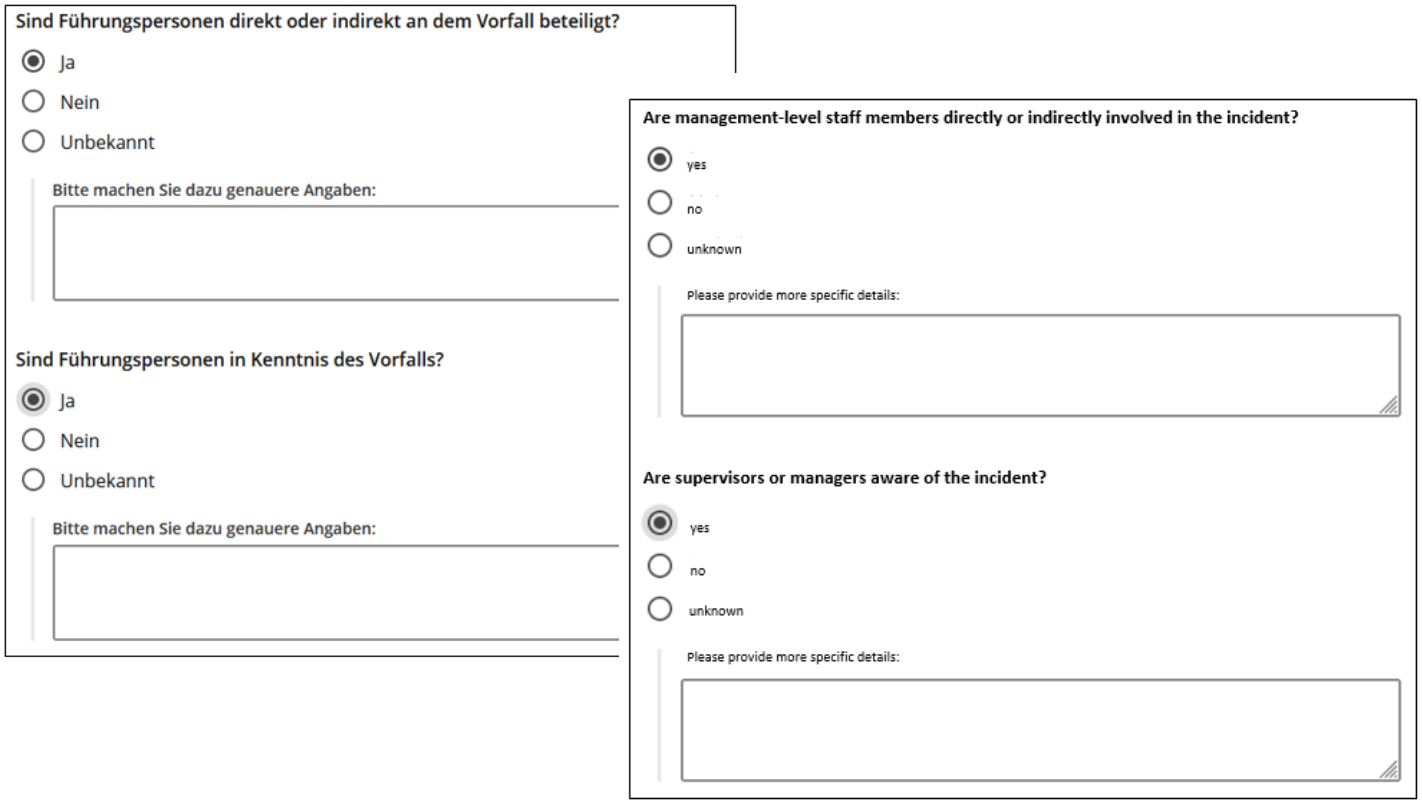
Are you an employee of the affected organisational unit?

- (•) yes
- ( ) no
- ( ) no information

Have you already reported the incident elsewhere?

- (•) yes
- ( ) no
- ( ) no information

Please provide more specific details:



Sind Führungspersonen direkt oder indirekt an dem Vorfall beteiligt?

- (•) Ja
- ( ) Nein
- ( ) Unbekannt

Bitte machen Sie dazu genauere Angaben:

Sind Führungspersonen in Kenntnis des Vorfalls?

- (•) Ja
- ( ) Nein
- ( ) Unbekannt

Bitte machen Sie dazu genauere Angaben:

Are management-level staff members directly or indirectly involved in the incident?

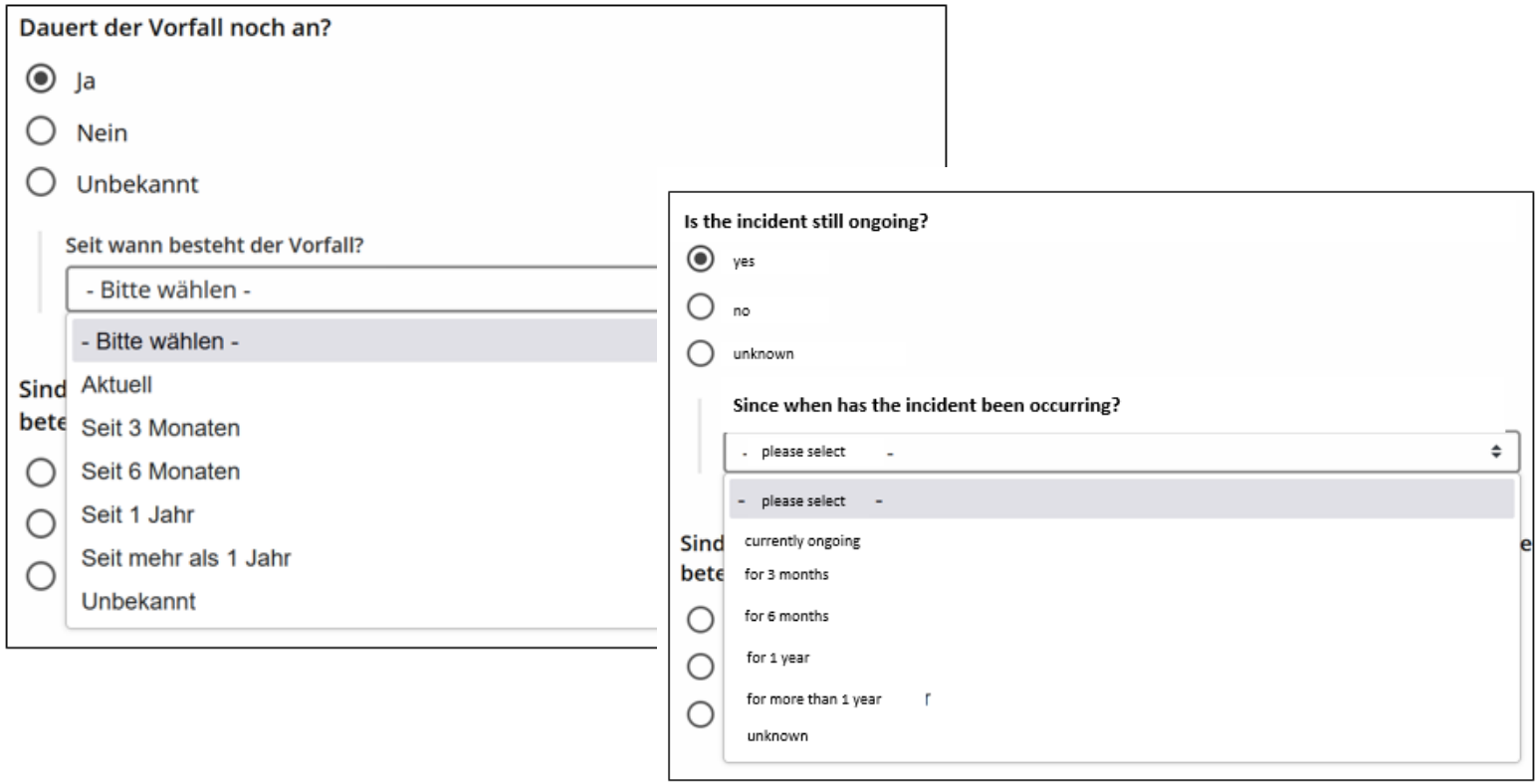
- (•) yes
- ( ) no
- ( ) unknown

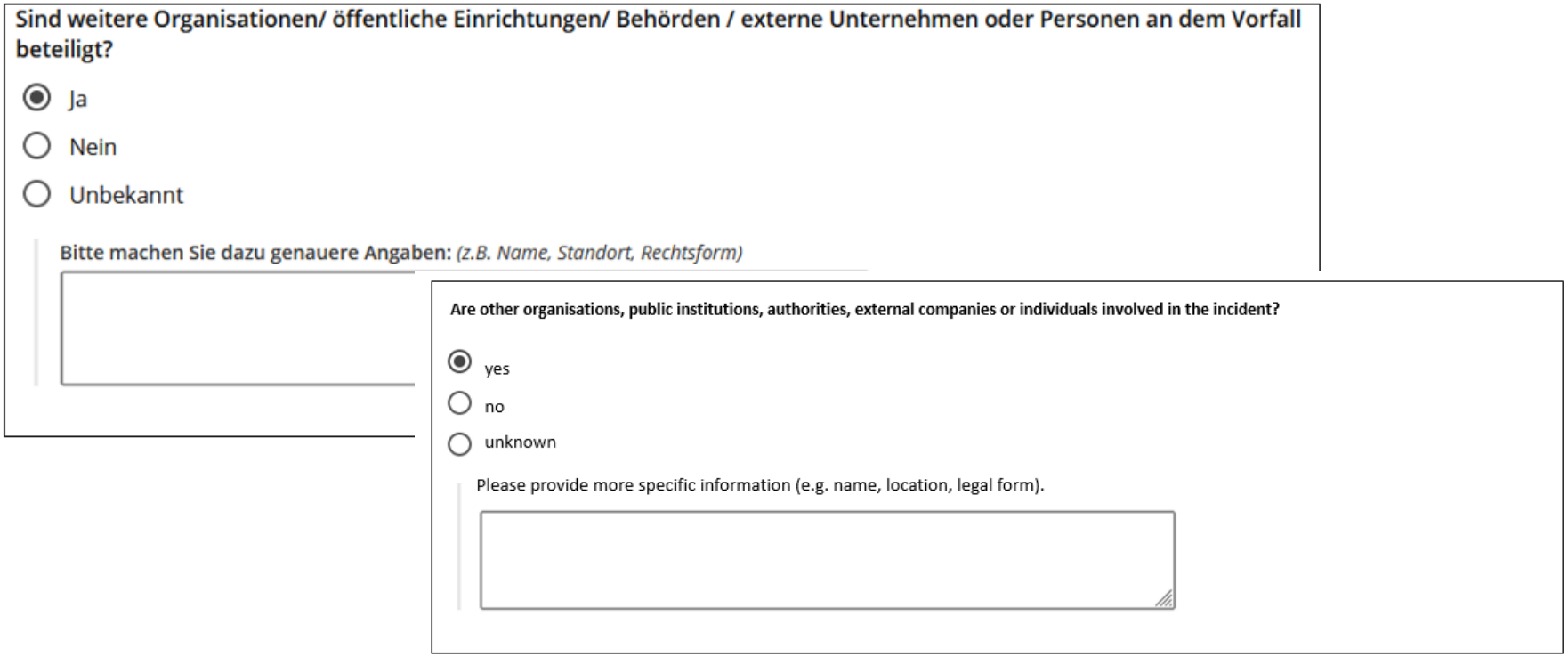
Please provide more specific details:

Are supervisors or managers aware of the incident?

- (•) yes
- ( ) no
- ( ) unknown

Please provide more specific details:


Dauert der Vorfall noch an?
Ja
Nein
Unbekannt
Seit wann besteht der Vorfall?
- Bitte wählen -
- Bitte wählen -
Aktuell
Seit 3 Monaten
Seit 6 Monaten
Seit 1 Jahr
Seit mehr als 1 Jahr
Unbekannt
Is the incident still ongoing?
yes
no
unknown
Since when has the incident been occurring?
- please select -
- please select -
currently ongoing
for 3 months
for 6 months
for 1 year
for more than 1 year
unknown


Sind weitere Organisationen/ öffentliche Einrichtungen/ Behörden / externe Unternehmen oder Personen an dem Vorfall beteiligt?
Ja
Nein
Unbekannt
Bitte machen Sie dazu genauere Angaben: (z.B. Name, Standort, Rechtsform)
Are other organisations, public institutions, authorities, external companies or individuals involved in the incident?
yes
no
unknown
Please provide more specific information (e.g. name, location, legal form).

Anhang: Sie können eine Datei bis zu einer Größe von 5 MB senden.

> **Hinweis zum Versand von Anhängen:** Dateien können versteckte personenbezogene Daten enthalten, die Ihre Anonymität gefährden. Entfernen Sie diese Daten vor dem Versenden. Sollten Sie diese Daten nicht entfernen können, kopieren Sie den Text Ihres Anhangs zu Ihrem Meldungstext oder senden Sie das gedruckte Dokument anonym unter Angabe der Referenznummer, die Sie am Ende des Meldungsprozesses erhalten, an die Anschrift des Hinweisempfängers (siehe Fußzeile).

☐ Hinweis zur Kenntnis ge

Durchsuchen... Keine Datei

Wenn Sie mehrere Dateien ü
Postkasten ein. Dort können

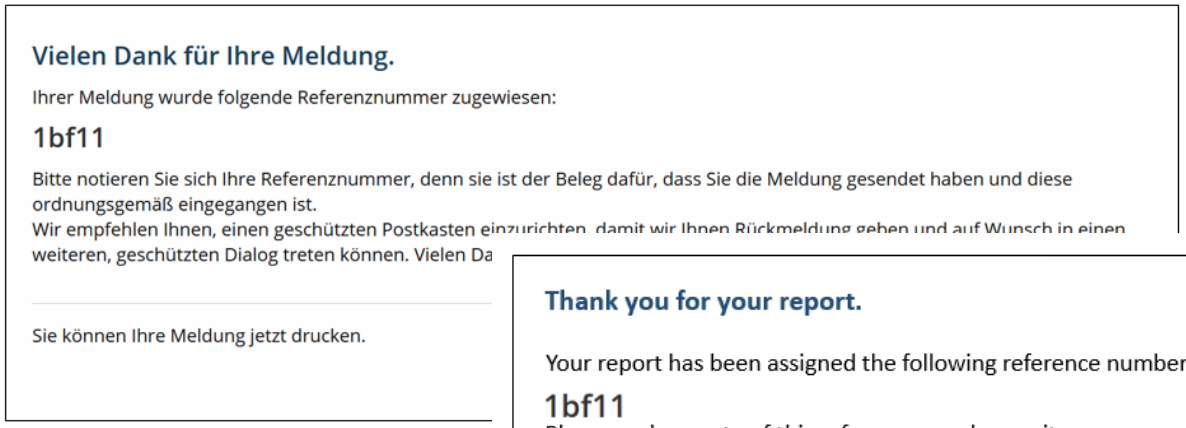
Attachment: You may upload a file of up to 5 MB in size.

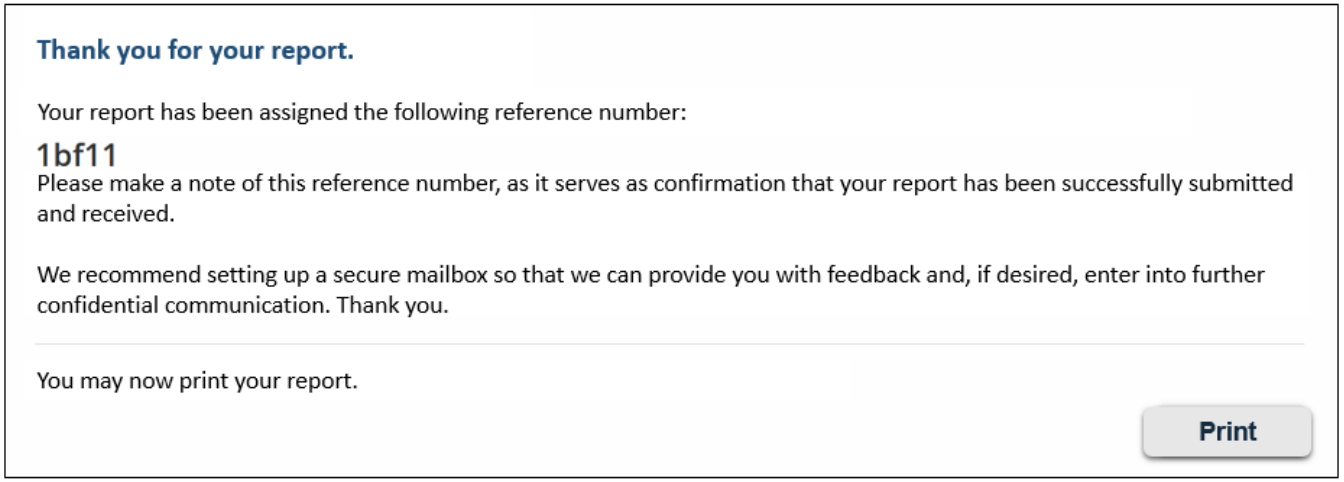
> **Notice regarding the submission of attachments:** Files may contain hidden personal data that could compromise your anonymity. Please remove any such data before submitting your files.
> If you are unable to remove this data, you may copy the content of your attachment into the message field or send a printed version of the document anonymously—quoting the reference number you will receive at the end of this reporting process—to the address of the designated recipient (see footer).

☐ Notice acknowledged.

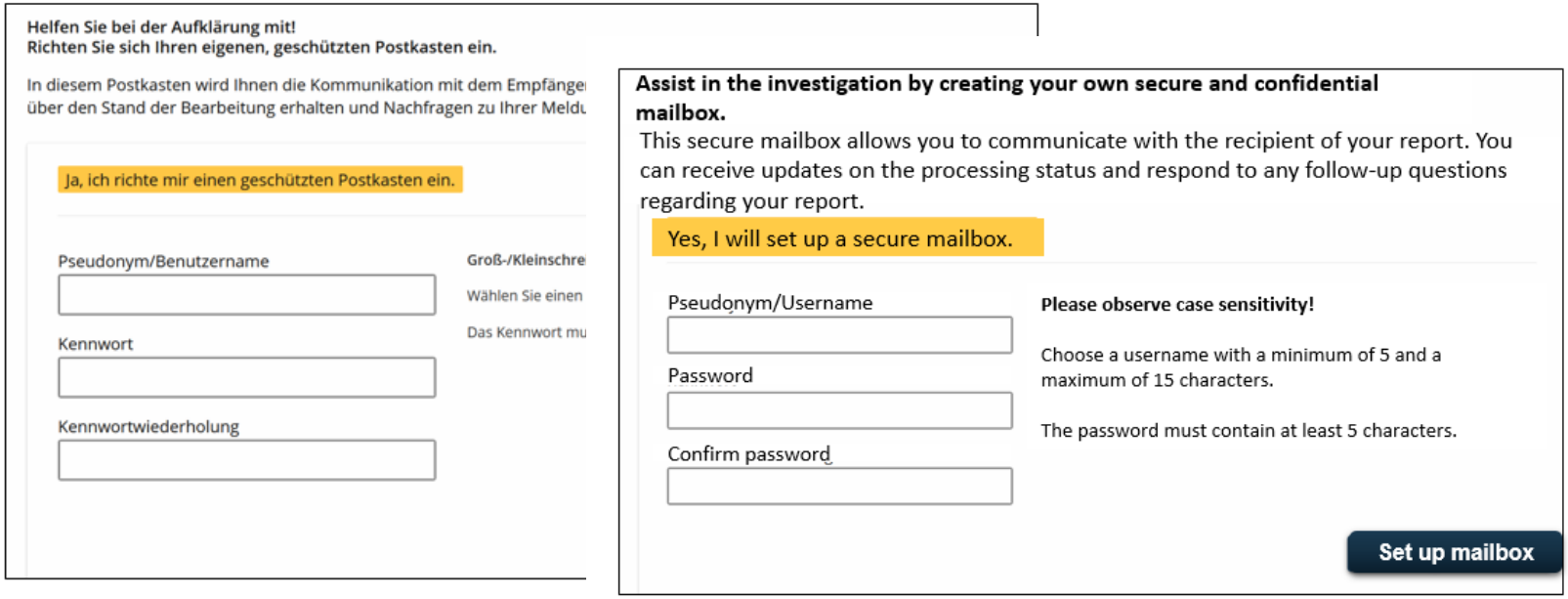
Durchsuchen... | No files selected.

If you wish to submit multiple files, please set up a secure mailbox at the end of this reporting process. You can then submit additional attachments as a supplement.





5) **After the report has been submitted, you will have the option to set up a secure mailbox. This secure mailbox allows you to communicate with the recipient of your report. You can receive updates on the processing status and respond to any follow-up questions regarding your report. If you choose not to set up a mailbox at this stage, the submission process will be completed at this point.**


Helfen Sie bei der Aufklärung mit!
Richten Sie sich Ihren eigenen, geschützten Postkasten ein.
In diesem Postkasten wird Ihnen die Kommunikation mit dem Empfänge
über den Stand der Bearbeitung erhalten und Nachfragen zu Ihrer Meldu
Ja, ich richte mir einen geschützten Postkasten ein.
Pseudonym/Benutzername
Groß-/Kleinschre
Wählen Sie einen
Das Kennwort mu
Kennwort
Kennwortwiederholung
Assist in the investigation by creating your own secure and confidential mailbox.
This secure mailbox allows you to communicate with the recipient of your report. You can receive updates on the processing status and respond to any follow-up questions regarding your report.
Yes, I will set up a secure mailbox.
Pseudonym/Username
Password
Confirm password
Please observe case sensitivity!
Choose a username with a minimum of 5 and a maximum of 15 characters.
The password must contain at least 5 characters.
Set up mailbox

Beachten Sie: Nur an dieser Stelle haben Sie die Möglichkeit, einen Postkasten einzurichten.

Merken Sie sich Ihre Zugangsdaten gut. Diese benötigen Sie für jedes Login in Ihren Postkasten. Ihre Zugangsdaten sind nur Ihnen bekannt und können daher bei Verlust nicht wiederhergestellt werden. Sie sollten Ihre Zugangsdaten sicher aufbewahren.

Nein, ich richte mir keinen Postkasten ein.

Please note: This is the only point at which you can set up a mailbox.

Please keep your access credentials safe. You will need them for every login to your mailbox. Your access credentials are known only to you and cannot be recovered if lost. Therefore, you should store them securely.

No, I do not want to set up a mailbox.

Finish

Vielen Dank für Ihre Meldung.

Sie haben sich entschieden, keinen Postkasten einzurichten.

Damit kann Ihnen Ihr Bearbeiter keine Rückfragen stellen und Sie nicht über den Stand der M
Auch in der weiteren Kommunikation über den Postkasten würden Sie anonym bleiben, solar
freiwillig bekannt geben.

Wenn Sie doch einen Postkasten einrichten möchten, klicken Sie jetzt auf „Postkasten einricht

Be

Thank you for your report.

You have chosen not to set up a mailbox.

As a result, your case handler will not be able to ask you any follow-up questions or inform you about the status of your report's processing. However, any further communication via postal mail will remain anonymous, provided you do not voluntarily disclose your personal information.

If you would like to set up a mailbox after all, please click on "Set up mailbox" now.

Finish

Set up mailbox

Technology
Arts Sciences
TH Köln

Privacy Notice for the Whistleblower System

The data controller responsible for the whistleblower system is:

Technische Hochschule Köln (TH Köln)
represented by the President, Prof. Dr. Sylvia Heuchemer
Claudiusstraße 1
50678 Cologne, Germany
Email: praesidium@th-koeln.de

If you have questions regarding data protection, you may contact our Data Protection Officers at:
datenschutzbeauftragter@th-koeln.de

The whistleblower system is operated on behalf of TH Köln by a specialized service provider:
EQS Group GmbH, Karlstraße 47, 80333 Munich, Germany.
TH Köln has concluded a data processing agreement with EQS Group GmbH in accordance with applicable legal requirements.

Purpose and Legal Basis of the Whistleblower System

The whistleblower system (BKMS® System) is intended to receive, process, and manage reports of legal violations in a secure and confidential manner, in accordance with the **Whistleblower Protection Act (HinSchG)**.

The legal basis for processing personal data is **Article 6(1)(c) of the EU General Data Protection Regulation (GDPR)** in conjunction with **Section 10 of the HinSchG**.

Version: 15. Juli 2025

Types of Personal Data Processed

When submitting a report via the whistleblower system to the internal reporting office, the following personal data may be processed:

- Your name, if you choose to disclose your identity
- Names and other personal data of individuals mentioned in your report

Information on the Use of the Whistleblower Portal and Anonymity

- Communication between your device and the whistleblower system is encrypted via **SSL**. SSL encryption ensures that data cannot be read or manipulated during transmission by verifying the validity of the website's certificate.
- Your **IP address is not stored** when using the whistleblower portal. A **session cookie** containing only a session ID is stored on your device to maintain the connection. This cookie is valid only for the duration of your session and becomes invalid once you close your browser.
- You have the option to set up a **secure mailbox** within the whistleblower system using a self-chosen pseudonym/username and password. This allows you to submit reports—either anonymously or by name—and to receive and respond to messages securely. All data remains within the whistleblower system and is particularly protected; this is not a standard email communication.
- You may also **attach files** to your report or when submitting additional information.
- If you wish to remain anonymous, please note that **files may contain hidden metadata** that could reveal your identity. Before uploading, remove such metadata. In most cases, you can remove metadata by right-clicking the file (e.g., a photo or document), selecting “Properties,” then the “Details” tab, and choosing “Remove Properties and Personal Information.”
- If you are unable to remove this information or are uncertain, you may copy the content into the report field or send a printed version anonymously, referencing the case number you will receive upon completion of the reporting process, to the address listed in the system footer.

Confidential Handling of Reports

Reports received are handled by the internal reporting office and treated with strict confidentiality. The office will assess the matter and may conduct further case-specific investigations. It operates within the **Internal Audit Department of TH Köln**.

During the investigation, it may be necessary to share the report and data concerning the individuals involved for further inquiries. All persons granted access to the data are—or will be—**individually bound by confidentiality obligations**.

Data Retention

Personal data will be retained only for as long as necessary to investigate and conclusively assess the report. After the conclusion of the process, the data will be **deleted after three years**, in accordance with legal requirements.

Rights of Data Subjects

In accordance with the **GDPR** and the **Data Protection Act of North Rhine-Westphalia**, both you and individuals named in your report have the right to:

- Access
- Rectification
- Erasure
- Restriction of processing

Please note that these rights are subject to a balancing of interests under the provisions of the Whistleblower Protection Act.

To exercise your rights, contact us at:
datenschutzbeauftragter@th-koeln.de

You also have the right to **lodge a complaint** with a supervisory authority. You may contact:
The State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia
(Contact details available at www.ldi.nrw.de)

Last updated: April 2025