CONFIDO

The Whistleblower System of the SHS Group

Reporting Violations of Laws, Guidelines and Human Rights

DILLINGER SHS - STAHL-HOLDING-SAAR saarstahl

Contact

Trust Center Compliance
SHS-Stahl-Holding-Saar GmbH & Co. KGaA
Building E22
Werkstraße 1
66763 Dillingen/Saar

confido@stahl-holding-saar.de

Free, Anonymous, International* Hotline
+800 / 44693473
Monday to Friday, 8 AM to 6 PM or by appointment
For USA calls: 01149 / 800 / 44693473
*For international calls please use a landline

Content

1. Whistleblower System

The SHS Group has implemented a whistleblower system with an internal reporting procedure in accordance with the Whistleblower Protection Act (HinSchG). Conduct that violates applicable law or company policies and thus does potentially cause damage to employees, the company or our business partners can be reported via the whistleblower system.

The whistleblower system can also be used as channel to submit complaints concerning the violation of human rights or environmental standards or complaints concerning related risks or violation of related obligations within the meaning of the Supply Chain Act (LkSG).

In line with our open and appreciative management culture, the supervisor should principally be the employees‘ first person to contact. Business partners can
contact the respective contact person in the group. But if this route appears inadvisable to you or ineffective you can use the whistleblower system.

As reporting alternative outsinde the group, the external reporting centre at the Federal Office of Justice can be used to submit reports of misconduct in a professional context.

1.1. Violations of Laws and Guidelines

The whistleblower system of the SHS group offers all employees, as well as external third parties, the possibility to report suspected violations of the law or serious violations of internal guidelines to the Trust Center Compliance. The incident must be related to the group, may relate to the economic activities of the group companies and/or to the individual behavior of a person within the group (see 8. Reporting Topics).

1.2 Violations of Human Rights

Likewise, the incident may involve a violation of human rights or a corresponding risk within the group‘s own business unit or at a direct supplier.

2. Trust Center Compliance

The function of the Trust Center is executed by the members of the Compliance
Committee, supported by the Compliance Analyst which has been defined by the Compliance Committee. The members of the Compliance Committee can act impartially and are not bound by instructions within the scope of the investigation. Contact details can be found on page 2.

3. Confidentiality

All provided reports and information – whether submitted anonymously or by name – will be treated strictly confidential by the Trust Center.

4. Whistleblower Protection

For the persons named in the reports, the accusations or suspicions can have considerable consequences, which is why the whistleblower system should only be used for serious, well-considered reports. The Whistleblower Protection Act (HinSchG) protects whistleblowers and prescribes uniform standards for their protection. The whistleblower system protects not only the whistleblowers themselves, but also third parties who are connected to the whistleblower (e.g. supporters of the whistleblower), as well as named witnesses and those affected by the whistleblowing. Further details can be found in the Whistleblower Protection Act.

5. Reports

Please make sure that you describe the reported issue as precisely as possible in the formulation of your concern – the more information is provided, the easier will the investigation be. You can base this on the five questions below:

- **Who? –** Who is involved in the reported circumstances?
- **What? –** What exactly happened?
- **When? –** When did this happen? How long has the problem been in existence
- already?
- **How? –** How did the reported circumstances come about?
- **Where? –** Where exactly did the incident happen?

Please also specifie if there are one or several persons who should not be contacted in the processing of your report under any circumstances.

6. Communication Channels

6.1. Written Report (Report Template)

Written reports can be sent by e-mail or by post to the Trust Center. The recommended method for whistleblowing is using the report template (see 10. Appendix). The questions in the report template guide along relevant data. The template is available in the SHS intranet as well as publicly accessible online at www.stahl-holding-saar.de under the category „Compliance“. The template should be possibly filled in electronically. This will help to avoid misunderstandings arising from misread handwriting. After completing it can be forward by e-mail or it can be printed out and send it by post.

6.2. Report by Phone

The Trust Center can be contacted by using a international, free, anonymous hotline +800-44693473.

This freecall universal telephone number assures the availablitiy from abroad and from Germany using a globally standardized telephone number format. The „+“ stands for the digits that must be dialed to set up an international call in the respective country. In many countries this is „00“, some countries have other dial-in numbers. Callers from Germany dial 00-800-44693473. Callers from other countries do not have to dial a country code - exception for the USA: 01149-800-44693473. Callers who use a group internal fixed telephone device must repect the peculiarities of the telephone system (e.g. possibly pre-dial the Zero to reach a number outside the group (0-00-800-44693473)).

The call is free of charge for callers, see also 9. FAQ, question no. 7.

The caller‘s number on the hotline is suppressed on the telephone display.

During the telephone call, all the information required to investigate the incident will be gained by the interlocutor. A telephone report is particularly recommended if the matter to be reported requires immediate processing, for example because there is imminent danger. A telephone report is the quickest way to initiate action.

6.3. Report in Personal Conversation

The Trust Center is also available for a personal meeting. An appointment can be made in writing or by telephone.

7. Anonymous Reports

Reports can be submitted anonymously. In this case, it is recommended that the notice is not handwritten and is sent by post without the sender‘s address. It should be borne in mind that it can be very helpful for the investigation of the incident if there is the possibility of knowing a contact person for queries.

8. Reporting Topics

8.1. Criminal or Improper Conduct

- Theft or unauthorized taking of items owned by the company or others
- Improper, non-compliant spending of company funds (e.g. the establishment of unregistered cash funds or accounts)
- Wilful destruction of company property
- Unauthorized, because prohibited or not approved, use of company property
- Forgery of documents such as invoices or contracts
- Serious contraventions of environmental laws (e.g. deliberate or grossly negligent pollution of water or soil by unprofessional, illegal dumping of harmful substances or chemicals, environmentally incompatible disposal of electrical appliances, rubbish dumping)

8.2. Anticompetitive Collusion & Agreements Contravening Antitrust Law

- Improper agreements (directly or via third parties, e.g. suppliers/customers/agents)
- with competitors about prices, pricing elements, market, customer or territory shares, about orders, production volumes and quotas or strategies
- Calls for boycott
- Exploitation of a monopoly position

8.3. Bribery, Corruption, Conflicts of Interest

- Undue influencing of business relationships or officials, e.g. by offering gifts or
- invitations
- Acceptance of personal advantages (for oneself and/or third parties) as a consideration for the non-compliance with internal rules and processes, e.g. order placement in circumvention of a due tendering process
- Preferring of friends and acquaintances in the placement of orders or selection of
- suppliers
- Engagement in activities that are in conflict with the employee‘s actual job, e.g. for a business partner whose commissioning is in the hands of the employee

8.4. Information Security

- Use of programs/systems to eavesdrop on persons (surveillance/tracking software, cameras, etc.) or for data espionage. This can be the case when hacking tools are used to identify passwords or in the targeted scanning of IT systems for vulnerabilities.
- Use of IT systems for illegal, unlawful activities or activities that are not authorized by the company. This can also include the use of company-owned equipment to access contents that have a pornographic, discriminating or criminal background, glorify violence or areliable to have an undesirable influence on the moral development of young people.
- Forwarding of confidential information to third parties (e.g. documents, passwords, company ID cards)
- Deliberate use of software that has not been properly licenced in a company environment
- Sharing in social networks of contents about the company that have not been released by the corporate communications department

8.5. Disclosure of Business and Trade Secrets

- This principally includes the surrender to unauthorized third parties of information of economic value that is either not public knowledge or not accessible to the public and has been confided to an employee as part of his or her job.
- This typically includes information about the following, e.g.:
  - Business strategies and other company data
  - Production processes
  - Inventions

8.6. Violations in Accountancy / Financial Reporting / Balancing of Accounts

- These can be encountered in all aspects of accounting, e.g.: Misstatement of turnovers, finances, inventories, expenditures, investments, unlawful cash, booking or bank transactions
- Establishment of slush funds for unlawful use in business transactions

8.7. Money Laundering and Terrorist Financing

- Deliberate and persistent ignoring of indications of money laundering.
- Acceptance of cash payments in business transactions
- Refraining from investigations despite engaging in business transactions with high-risk partners or politically exposed persons who refuse to disclose their economic beneficiary
- Acceptance of payments from third parties without verifiable attribution to the business partner

8.8. Product Safety and Product Conformity

- Deliberate creation of false or counterfeit certificates, application of incorrect labels
- Not informing the corresponding bodies in the company and concealment from the customer despite clear indications of health and safety risks posed by a product

8.9. Violations of Human Rights

- Violence, harassment, discrimination or disadvantaging at the workplace
- Reliance on forced and child labour (e.g. by suppliers)
- Violation of national, social occupational health & safety standards
- Withholding of an appropriate wage (usually the minimum wage)
- Disregard of the right to form trade unions or employee representatives
- Denial of access to food and water and unlawful deprivation of land and livelihoods

9. FAQ – Frequently Asked Questions

9.1. Questions

1. Why should I report an incident?
2. On which topics can I submit a report?
3. Which topics is the whistleblower system not intended for?
4. Do I need to inform my supervisor before reporting an incident?
5. How can I report an incident (internally or externally)?
6. Do I incur costs if I contact the Trust Center by telephone?
7. From which countries can the hotline be reached?
8. How should I contact the Trust Center if I am in a country from which the hotline cannot be reached (see question 7)?
9. Can I report an incident anonymously? Which way of reporting offers the greatest possible anonymity?
10. What happens once I have made my report?
11. Will my identity and other information provided by me be disclosed to external bodies?
12. Will my identity and other information provided by me be disclosed to the persons involved in the incident?
13. Can I enter into a dialogue with the Trust Center after submitting the report?
14. Can I demand information on the progress of the proceedings or result of my report?
15. Who can I turn to if I feel being targeted by reprisals?
16. What can I do if I am unjustly accused of misconduct?

17. How is it ensured that reports submitted per e-mail can only be read by the Trust Center?
18. What can I do if I am not certain if my concern is an issue for the whistleblower system?

9.2. Answers

1. Why should I report an incident?

Your report will help detecting irregularities early on, enabling the SHS Group to take action – ideally – before any damage occurs, if at all possible. You are thus contributing to the sustainable success of the SHS Group.

2. On which topics can I submit a report?

You can report all serious infringements of applicable laws, internal procedures or compliance guidelines. Relevant issues are listed below (not exhaustively).

- Human rights
- Bribery and corruption
- Anti-competitive agreements & agreements in violation of antitrust law
- Conflicts of interest
- Data protection
- IT security
- Protection of confidential information
- Behaviour indicating other offences such as fraud, breach of trust, embezzlement, theft, property damage
- Bookkeeping / financial reporting / accounting
- Money laundering and terrorist financing
- Product safety and conformity

3. Which topics is the whistleblower system not intended for?

The whistleblower system is not intended for:

- General complaints (dissatisfaction with operational processes, disagreements within departments, etc.)
- Customer service (product queries, complaints about defects, etc.)
- Emergencies (in an emergency, please contact the plant security or similar emergency call centres immediately)
- Minor violations of internal regulations (work errors)
- General questions to the Compliance Committee (Please contact: coko-info@stahl-holding-saar.de)

4. Do I need to inform my supervisor before reporting an incident?

In line with our open and appreciative management culture, the supervisor should principally be the employees‘ first person to contact. But if this route appears inadvisable, it is possible to contact the Trust Center directly. Business partners can contact the respective contact person of the group company.

5. How can I report an incident (internally or externally)?

Within the group, the incident can be reported to the Compliance Committee written by post or by mail, by telephone or during a personal conversation.
Recommended is to use the report template so that the report can be duly processed and investigated. The template can also be used as orientation in case a personal conversation (telephone, personal meeting) with the Compliance Committee is prefered.
If the template is not used, it should be made sure that all the aspects mentioned in the report are detailed. It is recommended to assign a unique ID number to every report (combination of the submission date and any four additional characters, e.g. 2023-10-15_h49s). This will enable the whistleblower to provide further information about an already reported issue (anonymously) in the future, or to make enquiries.

As reporting alternative outsinde the group, the external reporting centre at the Federal Office of Justice can be used to submit reports of misconduct in a professional context.

6. Do I incur costs if I contact the Trust Center by telephone?

No, there are no costs for the caller.

7. From which countries can the hotline be reached?

The hotline of the Trust Center can be reached from the following countries, there are no costs for the caller.

- Belgium
- China
- Germany
- France
- Italy
- Malaysia
- The Netherlands
- Poland
- Sweden
- Switzerland
- Spain
- Czech Republic
- Turkey
- United Kingdom
- USA (Achtung: Vorwahl notwendig: 01149 / 800 / 44693473)

8. How should I contact the Trust Center if I am in a country from which the hotline cannot be reached (see question 7)?

People from countries from which the free hotline cannot be reached should contact the Trust Center by e-mail.

9. Can I report an incident anonymously? Which way of reporting offers the greatest possible anonymity?

If your report is not handwritten and is mailed without a return address, your identity of the whistleblower will not be technically traceable. Please make sure that you provide all essential information on the circumstances in this case. This will be easier if you use the report template. You could fill it in on the PC, print it out, and send it to the Trust Center without return address.

10. What happens once I have made my report?

Your report will be documented in accordance with the law by the Trust Center, that was specifically established for this purpose, and then processed, possibly with the involvement of other departments.

11. Will my identity and other information provided by me be disclosed to external bodies?

Your personal data will only be provided or disclosed to external bodies insofar as this is required by a legal structure, or serves the legitimate interest of a SHS group company or external body. In all these cases, this disclosure needs to accord with data protection regulations.

12. Will my identity and other information provided by me be disclosed to the persons involved in the incident?

Your report will always be treated confidentially. The protection of the whistleblower, who does not report incorrect information through gross negligence, has top priority. The persons concerned (e.g. persons mentioned in your report, e.g. potential accused, third parties) must be informed of the processing of their personal data for data protection reasons according to the Whistleblower Protection Act (HinSchG) and other legal regulations. But if there is a significant risk that this disclosure could jeopardize the effective investigation of the issue, it can be postponed for as long as this risk applies. The identity of the whistleblower will only be disclosed after a so called weighing of legally protected rights, meaning that it will not be disclosed if the legitimate interest of the whistleblower prevails. If the investigation leads to the institution of criminal proceedings, however, the accused is due a right of access to documents. in this context, the accused can also find out the name of the whistleblower on the basis of statutory regulations.

13. Can I enter into a dialogue with the Trust Center after submitting the report?

Yes, you can always contact the Trust Center directly. If you have assigned an ID number to your initial report, stating it will facilitate a faster entry into the subject matter.

14. Can I demand information on the progress of the proceedings or result of my report?

Yes, you can contact the Trust Center with questions about the development of the case after the conclusion of the internal investigation.

15. Who can I turn to if I feel being targeted by reprisals?

In this case, please contact the Trust Center. However, you should also ensure your own protection by contacting the Trust Center, preferably at short notice, directly and without informing third parties in advance. This will prevent people who are not subject to the obligation to protect whistleblowers from taking inappropriate and undesirable measures.

16. What can I do if I am unjustly accused of misconduct?

Please contact the Trust Center. If the system is deliberately abused, the whistleblower cannot invoke protection by the system. The whistleblower‘s identity can be disclosed in this case to assert own legal claims against him or her.

17. How is it ensured that reports submitted per e-mail can only be read by the Trust Center?

Generally, third parties – external or internal – do not have access to your mailbox, unless you have explicitly passed these rights to internal colleagues (sharing). For technical reasons it is necessary that few system administrators can access the central e-mail system “Exchange” (maintenance, fault clearance). However, this access and the rights are highly regulated technically and organizationally.
Access to individual mailboxes is generally prohibited. Approvals for access by special administrators require, among other things, the approval of the independent group data protection officer. Violations of the regulations are taken very seriously and are punished.

18. What can I do if I am not certain if my concern is an issue for the whistleblower system?

Please contact the Trust Center in this regard. Your enquiry will be treated as confidentially as the report itself.

10. Appendix – Report Template

Report template

Whistleblower system of the SHS Group

If you wish to submit a report that indicates serious violations of laws or guidelines that have been or are being committed by members of the SHS Group or by third parties who have a business relationship with the companies of the SHS Group and who are or will be in business connection with them, please use the present template.

You can send the completed template either scanned by e-mail or by postal mail to the following addresses:

E-mail: confido@stahl-holding-saar.de

Address: SHS-Stahl-Holding-Saar GmbH & Co. KGaA
Trust Center Compliance
Building E22
Werkstraße 1
66763 Dillingen / Saar

Report template

Please also note the following **data protection information** on pages 4 - 6.

The fields marked with * are mandatory.

1. Personal details (Do not fill in if you want to submit an anonymous report.)			
Last name	First name	E-mail	Other, preferred method of contact

2. In which country did the incident take place?

3. When did the incident take place? *	4. Does the incident still continue? *

5. For employees only	
5a) Have you informed your supervisor? *	5b) Is your supervisor involved in the incident?

6. Have you - as an external third party - informed other people about the incident?

7. Do you have any relevant information about the incident or can you name someone who might have such information?

8. Would you like to warn us - whom we are not allowed/should not contact for clarification of the incident under any circumstances, in order not to endanger your anonymity?

9. Description of the incident and the persons involved. *

Data protection information as per GDPR section 13

This data protection information informs you about the processing of your personal data by SHS - Stahl-Holding-Saar GmbH & Co. KGaA in the whistle-blower system. According to section 4.1 of the GDPR (General Data Protection Regulation), your personal data include all information relating or relatable to you as a person, especially by reference to an identifier such as a name, or to an organization or personnel number enabling you to be identified.

Personal information and personal data

In the reporting attending the whistle-blower process, the trust centre collects and processes in-formation (both in paper and digital form).

These data may include all the data that you have reported or that become known in the further processing of the case:

- Master data (name, private or business address, telephone number, gender, e-mail address)
- Contract data (employment type, pay scale, employment level, employment start/end)
- Organization data (job name, supervisor, location, management level).

Using our whistle-blower system does not oblige you to provide your personal data. But the pro-vision of your personal data would enable us to ask further questions and investigate the report-ed incident more quickly. If you do not disclose any personal information to us, we may be forced to discontinue the investigation of the incident due to incomplete or faulty information.

Purposes of the data collection and processing

SHS - Stahl-Holding-Saar GmbH & Co. KGaA will only collect, process and use your personal data for dealing with reports of actual or possible crimes, administrative offences, and serious, persistent infringements of internal regulations insofar as there is a legal basis for this, with the objective of uncovering the misconduct of staff of the Saarland's steel industry (see https://www.dillinger.de/d/de/corporate/dillinger/gruppe/index.shtml and https://www.saarstahl.de/sag/de/konzern/index.shtml) and its business partners, and of containing and/or correcting the negative consequences of this misconduct for the SHS Group, its institutions, facilities and assets.

Please see below for the purposes including the legal basis:

- Contacting you if we have further questions after your report (e. g. on the subject of your concerns, time and duration of the incident, business unit, circumstances of you gaining knowledge of the incident, possible substantiating documents and proofs), GDPR sections 6.1.a & f
- Answering your general queries concerning the reported circumstances, GDPR sections 6.1.a, c & f
- Forwarding to suitable internal bodies for the investigation (e. g. company management, the group's internal auditing department, personnel, IT, legal and data protection departments), GDPR section 6.1.f
- Forwarding to the persons concerned to fulfil their right of access, GDPR section 6.1.f

- Forwarding to persons bound by professional secrecy (lawyers) or other third parties contractually bound to maintain confidentiality for the further investigation of the reported incident, and possible assertion of civil claims against the reported persons. Forwarding to law enforcement agencies for law enforcement purposes in case of criminally relevant acts by the reported persons, GDPR sections 6.1.c & f, Federal Data Protection Act section 28
- Prosecution of fraudulent reports, GDPR section 6.1.f

We will only process your personal data within the framework of the stated purposes and insofar as required for them

Consent

By sending your report, you are also consenting to SHS - Stahl-Holding-Saar GmbH Co. KGaA processing and storing the personal data provided by you therein for the purposes stated in this data protection declaration, including the purpose of investigating any incident reported by you. You further consent to the personal data also being processed over and beyond the conclusion of an investigation for as long as required for an appropriate evaluation of the incident with re-spect to the further proceedings.

You can withdraw your consent anytime with effect for the future. Please address your revocation to our data protection officers (see below).

Your data protection rights

Your data protection rights are enshrined in GDPR chapter III (sections 12 ff.). These regulations entitle you to access the personal data stored about you, and be informed of the purposes of their processing, their possible disclosure to other bodies, and the storage period.

To satisfy your right of access, you can also be provided with excerpts or copies. If data should be inaccurate or no longer required for the purposes they were collected for, you can demand their rectification, deletion, or a restriction of their processing.

If your particular situation provides reasons not to process your personal data, you can object to such processing insofar as it is based on a legitimate interest. In this case we will only process your data if there are compelling legitimate grounds for this.

Disclosure of your personal information

We will not forward your data to third parties as a matter of principle, and will only disclose them to third parties without your consent if we are required to do so by law or based on a court or authority decision. In individual cases, your personal data can be disclosed to law firms commissioned by us.

Controller of the processing of your personal data

The controller of the collection, processing and use of your personal data is SHS - Stahl-Holding-Saar GmbH & Co. KGaA, Werkstrasse 1, 66763 Dillingen/Saar, Germany.

The personnel data are stored and processed in the digital databases of the trust centre on the servers of SHS - Stahl-Holding-Saar GmbH & Co. KGaA. The concept and technical installation are designed to ensure that only a restricted group of specially authorized people are authorized to access them and that any other access or other gaining knowledge of the data is excluded in keeping with the state of the art and internal specifications.

Complaints about the processing of your personal data

If you have reservations or questions about the processing of your personal data and information, you have the right to lodge a complaint with a supervisory authority, in particular in the member state of your habitual residence, place of work or place of the alleged infringement. You can turn to the trust centre or your respectively responsible data protection officer as a first contact.

Data protection officer contact data:

Mr Philipp Paquet
Data Protection Officer
Bismarckstraße 57-59, 66333 Völklingen
Tel.: +49 6898 102124
Fax: +49 6898 104040
E-Mail: Philipp.Paquet@stahl-holding-saar.de

Storage period

The trust centre processes personal data for as long as their knowledge is required to meet statu-tory requirements, or for the purposes of the investigation, or for the possible subsequent appli-cation of measures under civil or criminal law to the persons involved. We base this on the statu-tory limitation periods under civil and criminal law in a case-by-case assessment. In addition to this we also store your personal data insofar as statutory retention periods apply in connection with a report. This can particularly play a role in circumstances of relevance under tax law where section 147 of the tax code requires a storage period of ten years for business letters in-cluding e-mails.