# Procedure description reporting concerns (whistleblower system)

## Introduction

The Basler group respects applicable law in the context of its business activities, the implementation of its strategy and the achievement of its goals and expects the same from its employees and business partners. In addition, the Basler group is committed to upholding its corporate values. The Basler corporate culture is also supported by the responsible and ethical actions of its corporate bodies, managers, and every employee. These principles are laid down in the Code of Conduct of the Basler Group. In order to ensure compliance with the Code of Conduct, the Basler group offers a whistleblower system with various reporting channels (for contact details see Annex) as a reliable way to report violations of the Code of Conduct, operational policies, or violations of the law (hereinafter referred to as "Reports").

This description describes the procedure for submitting and handling Reports. It is intended to ensure that Reports are received in accordance with the requirements of the Code of Conduct as well as data protection and data security, and that they can be processed, stored and archived with the necessary confidentiality in compliance with the law.

Where local regulations are stricter than the minimum standards set out in this procedure, the stricter rules shall apply in each case. If there is a conflict between relevant laws and this Policy, the affected company shall inform the Compliance Team in order to resolve the conflict.

This procedure does not oblige anyone to provide information. However, if there are legal, contractual or other duties or obligations to provide information provide Reports, these shall remain unaffected.

This procedure applies worldwide to all corporate bodies, employees and third parties.

## Notes

All corporate bodies, executives and employees of the Basler Group and third parties are entitled to submit Reports.

The whistleblower system is used exclusively for reporting violations of the Code of Conduct, company procedural principles or legal violations in an operational context. It is not intended for the submission of general complaints or for product or material compliance concerns or warranty inquiries.

Information may only be provided if the person providing the information believes in good faith that the facts he or she is reporting are true. In particular, it is not in good faith if he or she knows that a reported fact is untrue. In case of doubt, relevant facts shall be presented not as a fact, but as an assumption, evaluation or as a statement of other persons. It is pointed out that a person making a Report may be liable to prosecution if, against his or her better

knowledge, he or she claims untrue facts about other persons. Furthermore, whistleblowers who do not act in good faith are not subject to protection against discrimination or reprisals.

## Reporting Channels

The submission of notices of actual or suspected violations shall be made possible orally, in writing, or in person as follows:

Information from corporate bodies, managers, employees and external persons can be reported to:

- Compliance Team
- Ombudsman
- via the EQS Integrity Line digital whistleblower system

Employees can also submit Reports via a mailbox at the Ahrensburg site.

The contact details of the above reporting channels are listed in the annex to this procedure description.

Employees may also contact their supervisor or specialized offices/special functions, e.g. representative for severely disabled persons, AGG representative, for advice and assistance in submitting information to the responsible offices.

If the alleged violation was committed by a person belonging to the competent bodies, the notification shall be made through one of the other competent bodies.

In the electronic system EQS Integrity Line, the types and 7 languages of the notification are technically predefined. In all other respects, however, the submission of Reports is not bound to specific forms.

The reporting channels and the procedure for Reports are designed in such a way that only the persons responsible for receiving, processing and handling Reports, investigations, measures and decisions have access to the Reports. This is generally the Compliance Team. However, if a whistleblower decides to submit a Report to the reporting channels by e-mail, the usual corporate rules for access authorizations are applied to ensure compliance with data privacy and security.

In addition to the above-mentioned internal reporting channels, external reporting points are also available for submitting reports. These are listed in the Sharepoint of the Basler group on the CoCo page Compliance as well as in the digital whistleblowing system EQS Integrity Line.

However, in cases where internal action can be taken effectively against a violation and no reprisals are to be feared, the internal reporting channels shall be preferred.

## Procedure for Reports

The process begins with the submission of a Report via one of the reporting channels. All Reports are forwarded to the Compliance Team and centrally documented in the electronic system EQS Integrity Line. If a Report is made via reporting channels other than the Compliance Team or the EQS Integrity Line digital whistleblower system, it is forwarded and documented only with the consent of the person providing the information.

The person making the Report receives an acknowledgement of receipt no later than seven days after providing the information, unless the person providing the information has not provided a means of contact or has not set up a secure mailbox for communication in the EQS Integrity Line electronic system.

The notice is generally reviewed by the Compliance Team. The Compliance Team ensures the appropriate and independent review. In special cases, if there is a specialized unit or special function within the Basler group, e.g. representative for severely disabled persons, AGG (equality) officer, data protection officer, the further procedure will be coordinated with this unit or handed over to it. Decisions on the conduct and evaluation of investigations, the involvement of special functions or specialized bodies and the taking of measures are made unanimously, avoiding conflicts of interest. They are documented in the digital whistleblower system in a traceable manner. The Compliance Team ensures the implementation of measures. Details are regulated by an internal process.

The person making a Report is entitled to be informed about the result of the examination of the case and any measures initiated or planned as a result, as well as the reasons for such measures, insofar as this does not affect internal inquiries or investigations or the rights of the persons who are the subject of the Report. This information shall be provided at the latest within 3 (three) months after confirmation of receipt. The foregoing shall not apply if the person making the Report has not provided a means of contact or has not set up a secure mailbox for communication in the EQS Integrity Line digital whistleblower system.

## Confidentiality, anonymity, data protection

To the extent permitted by law and insofar as this is compatible with the conduct of an adequate investigation, the Basler Group protects the confidentiality and anonymity of the person making the Report. In particular, the use of the digital whistleblower system EQS Integrity Line does not allow any conclusion to be drawn as to the identity of the person providing the information. In the same way, confidentiality applies with regard to the persons who are the subject of a Report or are named in a Report. The authorization concept, including access matrix, which is to be maintained properly and updated at all times, is used to record which persons may

access the Report and the associated data and which rights they have within the scope of the processing.

All information, regardless of its truthfulness, is liable to damage the reputation of the persons concerned, the persons providing the information and/or third parties, and the Basler Group. They will therefore be treated with special confidentiality over and above the obligations arising from the data protection laws.

Data is generally deleted after three years following the conclusion of the procedure and after deletion approval by two members of the Compliance Team. To comply with legal requirements or in the case of existing legitimate interests of Basler, documentation may be kept longer as long as this is necessary and proportionate. Only the information recorded in the case register is exempt from deletion and is used for evaluation purposes. This does not include any personal information.

## Protection against discrimination

No whistleblower shall suffer reprisals, retaliation or other negative consequences as a result of making a Report. The Basler Group undertakes to prevent and, if necessary, to punish any repressive or discriminatory actions against the whistleblower. This does not apply if the whistleblower was actively involved in the reported violation.

Boards, managers and employees who take reprisal, retaliatory or other adverse action against an individual who has made a good faith Report will be subject to disciplinary action, up to and including termination.

The improper reporting of false information is not subject to the protections of this section.

## Annex 1 to the Procedure description reporting concerns (whistleblower system)

## Contact details reporting channels

### Compliance Team

- E-Mail: Compliance@baslerweb.com

- Members:
  - Hardy Mehl, Chief Executive Officer
  - Jan-Marek Pfau, Executive Director Human Resources & Organizational Development
  - Mahmud Nesredin-Said, Organizational Project Manager, Chairman Central Work Council
  - Birgit Braaker, Head of Legal (compliance manager):

### Ombudsmann

- Lawyer Stefan Nau, Kanzlei Segelken & Suchopar, nau@sesu.de, T +49 30 226287-0

### Electronic whistleblowing system

- EQS Integrity Line: https://baslerweb.integrityline.app/ [1]

### Letter Box

- at the Ahrensburg site with the label "Hinweise Compliance", location plan published on the Compliance page in Sharepoint

[1] [1] If you want to ensure anonymity
- Do not create the report from your employer's computer.
- Do not use a PC connected to the company network/intranet.
- Access the reporting system by typing the URL address directly into the browser and not by clicking a link.
- Do not write personal data in the report.