

Policy
for the establishment and operation
of a whistleblower system
in XY Company

Contents

- 1. Preamble 3**
- 2. Scope of application 3**
 - 2.1 Personal scope 3
 - 2.2 Substantive scope 3
- 3. Submission of a report..... 3**
 - 3.1 Definition of a report 3
 - 3.2 Open, confidential or anonymous reports 4
 - 3.3 Limits of confidentiality..... 4
 - 3.4 Content of the report..... 4
- 4. Reporting channels 4**
 - Reporting channels in an individual company 5
 - 4.1 Ombudsman’s office 5
 - [Optional: 4.2 Compliance officer 5
 - Reporting channels in a corporate group 6
 - 4.1 Ombudsman’s office 6
 - [Optional: 4.2 Compliance officer 6
 - 4.3 Reporting to government agencies 7
- 5. Procedure sequence following submission of a report..... 7**
 - 5.1 Report submitted to the ombudsman’s office 7
 - 5.1.1 Confirmation of receipt 7
 - 5.1.2 Carrying out an investigation 7
 - 5.1.3 Informing the whistleblower about the outcome of the investigation 7
 - 5.1.4 Reporting of reports received 7
 - 5.2 Submission of reports to the compliance officer 8
- 6. Protection of the whistleblower and the persons involved in the investigation 8**
- 7. Protection of the person incriminated in the report..... 8**
 - 7.1 Right to information..... 8
 - 7.2 Right to comment..... 8
 - 7.3 Right to deletion of data 8
- 8. Misuse of the whistleblower system 8**
- 9. Further rights of data subjects 9**
 - 9.1 Right to information..... 9
 - 9.2 Right to correction, blocking or deletion 9
 - 9.3 Notification of the recipient..... 9
 - 9.4 Assertion of rights 9
 - 9.5 Right of objection 9
- 10. Rights to appeal..... 9**
 - 10.1 Infringement of this policy 9
 - 10.2 Right to examine the outcome of the investigation 9
 - [Optional, if a works council is present: 10.3 Involvement of the works council 10
- 11. Implementation/Responsibility 10**
- 12. Data protection 10**

1. Preamble

Company XY has established secure reporting channels to enable its employees to report significant misconduct that is directed against *Company XY*, its employees or its partners.

In addition to the possibilities that existed previously and continue to be available of approaching supervisors, company management or a compliance officer in confidence with reports or suspicions of infringements of the law, the whistleblower system is intended to provide a further channel for communication. This whistleblower policy has been created to ensure the protection of whistleblowers and describes the procedure by which reports are received, checked and handled.

This whistleblower policy ensures that the statutory requirements for the protection of whistleblowers and for the handling of reports are complied with.¹

2. Scope of application

2.1 Personal scope

This whistleblower policy applies for all employees of *XY Company* (hereinafter: the '**company**') and temporary workers assigned to the company. This includes all members of the company management, all employees, all interns, all apprentices and all trainees.²

These persons are entitled to submit reports and on doing so they fall into the scope of protection of this policy.

2.2 Substantive scope

A report falls into the scope of the whistleblower policy where there is the necessity to report suspicion of an offence related to professional activity.³ This includes in particular offences to the detriment of the company, to individual employees or to partners of the company and their employees. Examples of offences include: insults⁴, bodily injury, abuse, sex crimes, corruption, theft, embezzlement, fraud, breach of trust and offences that involve infringement of laws on the protection of employees.

Other than this, a report falls within the scope of the whistleblower policy where actions that are punishable by a fine are reported, where the violated provision protects life, limb or health, the rights of employees or their representative bodies (works council), and in cases of infringement of EU law.

3. Submission of a report

3.1 Definition of a report

For present purposes a report is a piece of information that relates to circumstances falling within the scope of this policy under section 2.

A report should only be submitted if the whistleblower is acting in good faith that the circumstances described by him are true and correct. He is not acting in good faith if he knows that the circumstances reported do not correspond with the facts.

¹ Status of editing: 01.12.2022. At the current time HinSchG-E has not yet come into force.

² The company can grant external third parties the possibility of submitting reports. There is however no obligation in law to do so. The current version of the policy is based on the future legal framework conditions, see section 16 para. 1 p. 1 HinSchG-E.

³ At present there is no obligation to submit reports. It should be noted that if an obligation to report is introduced, the policy shall be subject to the co-determination of the works council.

⁴ If it is intended that the materiality threshold be set higher, the choice of offences can be changed, e.g. 'insults' can be deleted.

In cases of doubt, such circumstances should be indicated not as facts but as assumptions, evaluations or hearsay.

3.2 Open, confidential or anonymous reports

Reports can be submitted openly, confidentially⁵ or anonymously.

- Open report: This type of report includes the name and contact details of the whistleblower. The report is submitted without the reporting office being obliged to treat information about the person of the whistleblower or the content of the report confidentially.
- Confidential report: This also includes the name and contact details of the whistleblower, but the whistleblower obliges the reporting office not to pass his name and/or other information about his person and/or the report to third parties or to do so only to specified third parties.
- Anonymous report: This includes a description of a situation but carries no information about the person of the whistleblower.

3.3 Limits of confidentiality

The reporting office may not treat information concerning the whistleblower in confidence if it is required by law-enforcement authorities for disclosure in criminal or administrative proceedings, including administrative fine proceedings or where the obligation to disclosure is established by a court decision. In such cases the whistleblower is notified in advance in writing, where this does not interfere with the investigations, enquiries or court proceedings.

As regards the third parties named in the report, the reporting office shall not ensure confidentiality where the breaking of confidentiality is legally required, e. g. due to imminent danger. Additionally, information concerning persons who are the subject of a report can be passed on if this is necessary so that follow-up action can be taken or there is an official request or court decision in this regard.

3.4 Content of the report

All reports should be as specific as possible. The whistleblower should provide information in as much detail as possible about the circumstances to be reported. A report should contain at least the following information:

- Subject of the report
- Background and description of the circumstances
- Information on the time and place of the incident
- Information on the persons involved
- Where available and lawfully obtained: documents, images and other evidence.

4. Reporting channels

[Note: If the policy is customised, care should be taken to ensure that the explanations for either 'Reporting channels in an individual company' or 'Reporting channels in a corporate group' are preserved. The rules under 'Reporting channels in an individual company' are relevant for an individual company, while those for 'Reporting channels in a corporate group'

⁵ It is not mandatory under the law for anonymous reports to be accepted and processed. We recommend that anonymous reports be permitted, however, as this increases the chances of non-compliance being uncovered.

apply for holdings or other forms of company groups with one or more subsidiaries that in turn employ more than 50 employees.]

Reporting channels in an individual company

4.1 Ombudsman's office⁶

The company has set up an ombudsman's office. This enables the identity of the whistleblower to be protected and the information provided by him, where so requested by the whistleblower, to be passed on without disclosure of his identity.

The ombudsman's office is operated from:

*Reporting office AB
Street, number
Post code, postal town
Telephone: 0123 46789*

[description of reporting office, e.g. an external and independent law firm].

Availability by telephone is guaranteed on working days (Monday to Friday) during normal office hours.

[Optional: Whistleblowers also have the use of a digital whistleblower system for submitting reports to the ombudsman's office. The digital whistleblower system can be accessed at [https:// ...](https://...)]

The ombudsman's office advises whistleblowers on all questions relating to the reports, for example:

- on assessing the circumstances that give rise to suspicion,
- on the potential consequences of a report,
- on potential consequences in civil and criminal law for the whistleblower if they were involved in the misconduct reported,
- on the potential consequences in the event of an error in the reporting of suspicious facts.

The ombudsman's office handles the reports in accordance with the procedural processes set out in section 5 of this policy.

[Optional: 4.2 Compliance officer⁷

There is also the possibility of submitting reports directly to immediate superiors or to the compliance officer.

The company compliance officer is:

...

A report may be submitted to the compliance officer in person or by e-mail to the following address:

⁶ If an employee of the company (e.g. compliance officer) assumes the function of the internal reporting office, the rules should be modified accordingly.

⁷ Note (if necessary): For legal reasons, confidentiality can only be guaranteed to a limited extent where a report is passed to a compliance officer.

...]

Reporting channels in a corporate group

4.1 Ombudsman's office

The ombudsman's office receives reports concerning all subsidiaries in corporation XY. Each report must indicate the subsidiary to which it relates.

The ombudsman's office enables the identity of the whistleblower to be protected and the information provided by him, where so requested by the whistleblower, to be passed on without disclosure of his identity.

The ombudsman's office is operated from:

*Reporting office AB
Street, number
Post code, postal town
Telephone: 0123 46789*

[description of reporting office, e.g. an external and independent law firm].

Availability by telephone is guaranteed on working days (Monday to Friday) during normal office hours.

[Optional: Whistleblowers also have the use of a digital whistleblower system for submitting reports to the ombudsman's office. The digital whistleblower system can be accessed at [https:// ...](https://...)]

The ombudsman's office advises whistleblowers on all questions relating to the reports, for example:

- on assessing the circumstances that give rise to suspicion,
- on the potential consequences of a report,
- on potential consequences in civil and criminal law for the whistleblower if they were involved in the misconduct reported,
- on the potential consequences in the event of an error in the reporting of suspicious facts.

The ombudsman's office handles the reports in accordance with the procedural processes set out in section 5 of this policy.

[Optional: 4.2 Compliance officer

There is also the possibility of submitting reports directly to immediate superiors or to the compliance officer.

The compliance officer of the [*customise*: group/company] is:

...

A report may be submitted to the compliance officer in person or by e-mail to the following address:

...]

4.3 Reporting to government agencies

In addition to the reporting channels described in this policy, the whistleblower is also free to report their suspicion to government agencies, noting however the limits imposed on this by the law in force.

The German federal government has set up an office for external reports under the Federal Office of Justice (Bundesamt für Justiz). This external reporting office is separate in organisational terms from the remaining scope of the Federal Office of Justice.

5. Procedure sequence following submission of a report

5.1 Report submitted to the ombudsman's office⁸

5.1.1 Confirmation of receipt

The whistleblower receives confirmation of receipt within seven days of submission of the report, where this is technically possible. [**Optional:** This is the case where for example the digital whistleblower system of the ombudsman's office is used.]

Once a report is received by the ombudsman's office, a first check is performed by the latter, particularly for whether there is evidence available that corroborates or disconfirms the information given. If the ombudsman's office is of the view that further investigations should take place, this is documented and the information – where this is desirable while ensuring confidentiality – is forwarded to the⁹ compliance officer.

5.1.2 Carrying out an investigation

The investigation of the suspicious facts that have been reported is performed as quickly as is reasonably possible. If a report turns out to be incorrect or if it cannot be sufficiently substantiated with facts, this is documented accordingly and the investigation halted. No consequences are caused to the whistleblower. The company will use the results of each of its investigations to improve its compliance management system.

5.1.3 Informing the whistleblower about the outcome of the investigation

Where return communication is possible, the whistleblower receives a response within three months of the confirmation of receipt concerning the status or outcome of the investigation.

This notification is made on the condition that it causes no detriment to either the investigation or the rights of the persons named in the report.

5.1.4 Reporting of reports received

[**Optional/customisable:** The ombudsman's office shall provide the compliance officer¹⁰ of the company with a written report, on a quarterly basis and for internal use, concerning the reports received. This report is restricted to the types and number of reports in the various categories and their processing status, plus the percentage distribution of the reports across the different categories.]

The company has the right to request reports related to specific incidents or circumstances.

⁸ If an employee of the company (e.g. compliance officer) assumes the function of the internal reporting office, the rules should be modified accordingly.

⁹ A measure of entrepreneurial leeway is available here; the recipient can also be the relevant company management. In a corporate group, a central contact person can be nominated. It should be noted that the supervisory obligation constitutes a management task, and therefore the handling of incoming reports must not entirely bypass the management (of the respective company concerned).

¹⁰ See previous footnote.

5.2 Submission of reports to the compliance officer

Where reports are submitted to the compliance officer, the reports are handled in accordance with the specifications in section 5.1 of this policy.

6. Protection of the whistleblower and the persons involved in the investigation

Any person who submits a report in good faith or who is involved in the investigation of a suspicion shall be protected from negative disciplinary consequences or other disadvantages in their professional context. Exceptions can apply where the person is involved in the compliance incident being investigated.

Any employee or supervisor who harasses, discriminates or otherwise behaves abusively towards a whistleblower or a person involved in the investigation of a suspicion shall be liable to disciplinary measures that in the most serious cases can lead to their dismissal.

7. Protection of the person incriminated in the report

7.1 Right to information

The person incriminated in a report will be informed in due course and in consideration of data protection guidelines of the allegations made against them, provided that such notification does not significantly impede the progress of the procedure for determining the circumstances. This notification shall be made after completion of the investigation at the latest.

7.2 Right to comment

The person incriminated in a report must be heard or given the opportunity to provide a written comment before conclusions are drawn that involve naming the person. After this, the persons authorised to take decisions shall decide the course of action necessary in the interest of the company.

7.3 Right to deletion of data

If the suspicion expressed in the report does not prove to be true, the person incriminated in the report has the right to have the data stored about them in this connection to be deleted.

8. Misuse of the whistleblower system

Reports must be submitted in good faith. If the examination of a report indicates that there is no justification for suspicion or that the facts are insufficient for a suspicion to be substantiated, whistleblowers who submitted their reports in good faith have no need to fear disciplinary action.

A different situation applies for whistleblowers who deliberately misuse the whistleblower system by submitting false reports. Such persons shall be subject to disciplinary action and may become liable for damages. Persons who deliberately misuse the whistleblower system by submitting false reports further have no entitlement to confidentiality.

9. Further rights of data subjects¹¹

9.1 Right to information

All persons whose data is processed within the context of handling the report (e. g. the whistleblower, the person incriminated in the report or the person involved in the investigation) have the right under article 15 GDPR to request information about the data stored about them and further information, for example about the purposes of processing or the recipient of the data.

9.2 Right to correction, blocking or deletion

All persons whose data is processed within the context of handling the report (e. g. the whistleblower, the person incriminated in the report or the person involved in the investigation) have the right to have incorrect data about them corrected, have the right to have their data completed, and have it blocked or deleted, provided that the provisions for this are present in article 16 et seq. GDPR. A request for deletion is authorised for example where the data has been unlawfully processed or if the data is no longer required for the purpose for which it was collected. This applies for example in the case provided for in section 9.3 of this policy.

9.3 Notification of the recipient

If the company has passed the data to a third party, it will notify the recipient of the data of the correction, deletion or blocking of the data in accordance with the statutory provisions.

9.4 Assertion of rights

The rights can be asserted against the data protection officer of the company.

9.5 Right of objection

Where data is processed on the basis of legitimate interests of the company, the data subject of that processing can lodge an objection to the processing of their data by the company at any time for reasons arising from their particular situation. The company will then either prove compelling legitimate grounds that permit the processing or will cease processing the data.

10. Rights to appeal

10.1 Infringement of this policy

Both the whistleblower and the person named in the report can, if they suspect a violation of this policy, apply to their immediate supervisor, the company management, the compliance officer or the ombudsman's office.

10.2 Right to examine the outcome of the investigation

Both the whistleblower and the person named in the report can apply to the contact person named in section 10.1 if they believe the investigations that have been carried out to be erroneous or inadequate or if in their view they have been unjustly disadvantaged within the framework of the investigation. In this case the actions necessary to review the matter shall be initiated and the complainant informed accordingly.

¹¹ 'Data subjects' here means persons whose personal data is processed in connection with the processing of a report.

[Optional, if a works council is present: 10.3 Involvement of the works council

The reported person can avail themselves of their right to appeal under sections 84, 85 BetrVG (Works Constitution Act) and consult the works council.]

11. Implementation/Responsibility

The company management [in the case of a corporate group: the parent company] is responsible for publicising this policy and for its implementation. This includes in particular informing all employees of the whistleblower system.

[In a corporate group: The responsibility and obligation for remedying a violation discovered by means of the whistleblower system lies with the management of the particular company affected.]

12. Data protection

Personal data is collected and stored in the course of this process. This data is handled in compliance with the applicable data protection legislation, in particular the GDPR. Only such data is collected and processed as is objectively necessary for the purposes of this policy.

The data obtained as a result of a report is stored separately from all other data stored by the company. It is ensured by means of appropriate technical and organisational measures that only the persons responsible are granted access to this data. This also applies for the data of the whistleblower. Data that has been collected in connection with a report and that is not relevant for the investigation is immediately deleted. Other than this, the data collected is deleted as soon as the purpose for its collection and storage no longer exists. In cases of misconduct within the meaning of this policy or of abuse of the whistleblower system that result in criminal, disciplinary or civil court proceedings, the period of storage may be prolonged until the legal conclusion of that proceedings is reached.

Persons involved in the proceedings, which may include the whistleblower himself, can apply to the company data protection officer at any time to check whether the rights existing under the relevant applicable provisions have been observed. Where a data subject believes that the company is processing the data other than in compliance with the applicable data protection law, he can lodge a complaint with the data protection supervisory authority.

Place, date