Whistleblower policy H.J. Hansen-Group

Latest updated November 2022

Background and purpose

The H.J. Hansen-Group provides a common group whistleblower reporting system to its employees, business partners and other partners. The reporting system meets the requirements for whistleblower schemes in accordance with the Act on the Protection of Whistleblowers (the "Whistleblower Act"). In the following, the H.J. Hansen-Group is referenced to as the "Group".

A whistleblower reporting system is an independent channel through which employees, business partners and other partners can report suspicions or specific knowledge of serious violations of the law or other serious matters in the Group.

The whistleblower reporting system must be seen as a supplement to the Groups management or HR, if mistakes or unsatisfactory conditions are detected that you want to draw attention to.

This whistleblower policy describes in more detail when you as an employee, business partner or other partner may use the whistleblower reporting system, what you can report, how a report is handled, rights for those involved, etc.

In addition to this information, Mazanti-Andersen Advokatpartnerselskab has composed a privacy policy, which specifically relates to the processing of personal data in connection with reports to whistleblower reporting systems. It can be found here.

Who may report by way of the whistleblower reporting system?

1.1 The whistleblower reporting system can be used if you are employed or previously employed in the Group, and this also applies to unpaid interns and student assistants. It does not matter which job function the person is contesting. The whistleblower reporting system can also be used by business partners and other partners.

2. **Who can be reported?**

2.1 The whistleblower reporting system must be used to report information and circumstances regarding violations of the law and serious misconduct committed by employees or other persons associated with the Group. Other people may for example be board members, shareholders, supervisory board members, consultants, suppliers, contractors, auditors, etc.

3. **Which conditions can be reported?**

3.1 The Group comply with the delimitation of the Whistleblower Act, according to which both violations of EU law, serious violations of Danish law and other serious matters can be reported, as long as it is related to persons associated with the Group, cf. above.

3.2 A report may for example relate to a suspicion of or actual knowledge of violations within the following areas:

- Money laundering and terrorist financing
- Protection of privacy and security of network and information systems
- Consumer protection
- Economic crime, such as embezzlement, theft, bribery, fraud and forgery
- Hacking, eavesdropping, recording conversations among others, etc.
- Violations of the Bookkeeping Act, tax legislation, etc.
- Violations of confidentiality
- Ignoring a statutory duty to act
- Violation of rules on the use of force
- Deliberate misleading of citizens and business partners
- Physical and psychological violence and sexual abuse or serious harassment, e.g., due to of race, gender, language, wealth, national or social origin, political or religious affiliation
- Disregarding professional standards, which e.g., could cause a risk to the safety and health of individuals
- Neglect to care
- More serious or repeated violations of the workplace's internal guidelines, e.g. regarding business trips, gifts and accounting
- Serious errors and serious irregularities associated with IT operations or IT system management.

The above is a non-exhaustive list of examples.

3.3 The whistleblower reporting system must not be used for reporting information of a trivial nature, or e.g., information regarding breach of internal guidelines on sick leave, smoking, alcohol, clothing, private use of office supplies, or breach of ancillary regulations such as e.g., non-compliance with documentation obligations. However, in the event of systematic violation, it may well lead to these otherwise less serious conditions being conditions that should be reported to the whistleblower scheme.

3.4 The whistleblower reporting system cannot be used to report in regards of the whistleblower's own employment, including conflicts between employees, collaboration difficulties or matters that fall within the industrial law system. However, serious harassment and sexual harassment are covered, just as collaboration difficulties are covered if they are assessed to be so serious that they pose a real risk to people's lives and health.

3.5 It is possible to report information about violations or circumstances that have taken place prior to the Group's establishment of the whistleblower reporting system.

4. How is reporting made?

4.1 The Group's employees, business partners and other partners may report in writing and anonymously by way of a digital solution provided by an external supplier, hence the report is not made directly to the Group.

4.2 The link to the whistleblower reporting system can be found here: https://nordicwhistle.whistleportal.eu/WhistleBlower/Form/465-339-2ef295f5fbd4499f8b131ccd89585812

4.3 Read more about the procedure for making a report in our guide to the whistleblower reporting system, which can be accessed here: https://www.hjhansen.dk/wp-content/uploads/2023/05/EN-Guide-to-use-of-whistleblower-scheme-H.J.-Hansen.pdf

4.4 A link to the whistleblower reporting system and the instructions for this can also be found on our intranet and website.

5. Who receives a report?

5.1 Information covered by a report will be received by the Group's legal adviser, Mazanti-Andersen Lawfirm (hereinafter the "Recipient"), which is an external and independent adviser.

5.2 When a report has been received:

- the Recipient will screen the report, including the level in the Group, that the reporting is concerning,
- the Recipient will confirm receipt of the report to the whistleblower,
- the Recipient examines the report thoroughly and assess the matter, cf. section 7.1,
- the Recipient will contact the Group for a dialogue about and with recommended reactions to the report, and
- the Group will make a final decision on the appropriate reaction of the report.

5.3 We have chosen this particular solution as we want to create the greatest possible comfort for the Group's employees, business partners and other partners in connection with a report.

6. Procedure when receiving a report

6.1 When a report has been received, an assessment is made as to whether the report is covered by the scope of the whistleblower scheme, cf. section 3.

6.2 If a report falls within the scope of the whistleblower reporting system, the Recipient will handle the report by initiating the necessary investigations and to recommend the relevant measures in connection hereto, cf. section 7.

6.3 If the report falls outside the scope of the whistleblower reporting system, the report will be rejected, and the report will therefore not be dealt within the frame of the whistleblower reporting system. In that case, the whistleblower will receive guidance on where the whistleblower internally may address its request in regards of the relevant matter.

7. Investigation of a report

7.1 When the Recipient has received the report, the Recipient is responsible for thoroughly investigating the report, carrying out follow-up and taking the necessary measures to be able to inform the Group correctly.

7.2 The Recipient must then prepare a report for relevant and competent contact persons in the Group. On the basis of the statement and recommendations, the Group will decide on the relevant measures and reactions, whether it is the initiating of internal investigations, notification to the authorities or other reactions with an employment law perspective or contract law nature.

8. Confidentiality and disclosure of information

8.1 The Recipient is subject to a specific duty of confidentiality with regard to the information in a report.

8.2 The specific duty of confidentiality applies only to information contained in a report. If a report gives rise to initiating of a case, the information collected in that connection hereto, will not be covered by the specific duty of confidentiality.

8.3 The specific duty of confidentiality implies that the Recipient, as a general rule, may not pass on information about the whistleblower's identity or other information that directly or indirectly may reveal this to anyone other than the Recipient's authorized employees, unless the whistleblower, after any dialogue in this regard, specifically consents in whole or in part to disclose information.

Without the whistleblower's consent, such information may only be disclosed to public authorities, and only if the disclosure takes place to counter violations or to ensure the right of the persons concerned to a defense (e.g., if the report leads to prosecution of the reported). In these cases, the whistleblower must be notified prior to disclosure, unless the notification will jeopardize related investigations or legal proceedings.

8.4 The specific duty of confidentiality shall not prevent the Recipient from passing on information that does not directly or indirectly reveal the whistleblower's identity, if the purpose is to follow up on the report or to counter the reported violation(s). The Recipient may thus e.g., share the information with relevant and competent contact persons in the Group to investigate whether the reported violation actually occurs or has occurred. It may also be relevant to share information about suspected violations for the purpose of follow-up or countermeasures, e.g., between group-affiliated companies.

8.5 The persons who become aware of the information in the report in connection with disclosure are subject to the same duty of confidentiality as the Recipient and the Recipient's authorized employees, and the persons concerned will be made aware of this duty of confidentiality in connection with any disclosure.

8.6 If the whistleblower has deliberately revealed his/her identity in connection with a publication, the specific considerations for protecting the whistleblower's identity no longer apply. Since the specific duty of confidentiality thus does not apply, information about the identity of the whistleblower etc. may in such cases be passed on within the frames that may otherwise apply.

9. Anonymity, protection against retaliation and other rights of a whistleblower

9.1 As a whistleblower, you have the right to remain anonymous throughout the process. The selected IT solution provides the opportunity to communicate anonymously with the Recipient.

9.2 A report may, however, be of a such nature that it may be difficult to investigate a matter thoroughly, without the whistleblower choosing to come forward and thus waive his/her right to remain anonymous. It is the whistleblower's own decision whether this should happen.

9.3 The whistleblower reporting system is intended to protect the whistleblower, among other against any form of reprisals or threats of or attempted reprisals that occur as a result of the whistleblower making a report. Retaliation must be understood as any form of unfavorable treatment or unfavorable consequence that occurs as a reaction of a report. It can, for example, be suspension, dismissal, demotion or non-promotion, transfer of tasks, transfer, reduction of salary, disciplinary measures, coercion, intimidation, harassment, discrimination, etc.

9.4 Being mentioned in a report may have significant consequences, and therefore it is required that the whistleblower is in good faith about the content of a report. A deliberately false report from a whistleblower, e.g., for reasons of harassment, may have criminal consequences for the whistleblower.

9.5 On the other hand, a whistleblower cannot be held liable for disclosing confidential information if the whistleblower had reasonable motive to believe that the information passed on in the form of a report were correct at the time the report took place, and that the announcements referred to serious violations of the law or other serious matters covered by the scheme.

9.6 On that basis, the whistleblower will not be responsible for having gained access to the information reported on. However, this assumes that the act does not in itself constitute a criminal offense – e.g., burglary.

10. Ongoing communication and deadlines

10.1 The Recipient handles the communication with the whistleblower by way of the whistleblower system.

10.2 According to the Whistleblower Act, a whistleblower must receive a receipt for a report no later than 7 days after submitting his/her report.

10.3 In addition, the whistleblower must as soon as possible and no later than 3 months from confirmation of receipt receive feedback, which means that the whistleblower - as far as possible - must be informed about the measures that have been initiated or are intended to be initiated and why the specific follow-up has been chosen. In connection with feedback, there may be information that may not be shared with the whistleblower, e.g. due to statutory confidentiality, personal data legislation, etc.

10.4 In addition to information about the chosen follow-up, the whistleblower must, as far as possible, also have information about the course of the investigation and the outcome, if this is possible within the applicable regulation.

10.5 If it is not possible, due to the circumstances of the case, to give final feedback before the end of the 3-month period, the whistleblower must be informed of this together with information on when further feedback can be expected.

10.6 As mentioned, a whistleblower may choose to come forward, and in that case it may be appropriate to e.g. physical meetings with the Recipient.

11. Confidentiality

11.1 The whistleblower reporting system is designed and handled in such a way that confidentiality is ensured in regard of the identity of the whistleblower and the affected persons who may be included in a report.

11.2 The IT system used to handle the whistleblower reporting system is subject to a number of strict security requirements that, among other things, ensure anonymity and confidentiality. It means that the person who makes a report by way of the whistleblower reporting system is and remains anonymous if desired. This also means that the system does not log IP addresses, that metadata is removed from any uploaded files, and that all data transmission and data storage is encrypted.

11.3 The Recipient is subject to a duty of confidentiality, and access restrictions have been established to all information relating to a report.

12. Registration of reports and processing of personal data

12.1 Reports received, including documentation included in the report, must be registered (stored systematically) to ensure that there is access to the reports and that, if relevant, it can be included as evidence in any subsequent legal proceedings. At the same time, the registration also ensures that any reports regarding the same matter are identified and may lead to further investigation of a matter. This registration takes place in the whistleblower system.

12.2 Reports are kept for as long as it is necessary and proportionate in relation to the effective and legal handling of the individual reported case as well as in relation to any other obligations. The Recipient will continuously assess whether storage is still necessary and proportionate.

13. External whistleblower reporting system at the Danish Data Protection Authority

13.1 According to the Whistleblower Act, the Group is responsible to inform its employees, business partners and other partners about the following external whistleblower reporting system, which can be used as an alternative to the Group's internal reporting system:

13.2 The Danish Data Protection Authority has established an independent and external whistleblower reporting system, where everyone has the opportunity to report information regarding various violations of EU law, serious violation of applicable law and other serious matters,

13.3 More information on how to report to the Danish Data Protection Authority's whistleblower reporting system can be found here.

13.4 The Group's employees, business partners and other partners have the freedom of choice as to whether a report is made to the Group's internal whistleblower reporting system or to an external reporting system. However, the Group encourages its employees, business partners and other partners to use the Group's own whistleblower reporting system in cases where the whistleblower considers that the incident can be handled by the Group.

13.5 The possibility of using either the internal or an external whistleblower scheme does not limit the usual freedom of expression of the Group's employees.

14. Protection of the whistleblower in case of necessary disclosure of information

14.1 The whistleblower scheme's protection of whistleblowers also applies to a whistleblower's disclosure of information in the following events;

- when the whistleblower, prior to disclosure, has made an internal as well as an external report or a direct external report, without the recipient of the report having taken appropriate measures in response to the report within the deadlines specified under section 10,

- when the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest, or

- when the whistleblower has reasonable grounds to believe that an external report involves a risk of reprisals, or if, due to the circumstances of the case, there is little prospect that the violation will be dealt with effectively.