Directive Whistleblower Protection Act

Omnicom Holding Germany

Table of contents

1. Introduction

1.1. Purpose of the Directive

Compliance with the law is the basis of all our activities and we understand honest, ethical and compliant behaviour as the basis of our corporate success. To this end, we have established certain internal guidelines in which we concretise rules of conduct for specific areas (e.g. our Human Rights Declaration, the Energy and Environmental Management System, the Code of Conduct and the Data Protection Policy).

We expect all employees not only to adhere to our high standards, but also to commit to them.

Nevertheless, there is a risk for every organisation that something will go wrong from time to time or that employees will unknowingly or knowingly behave unethically or illegally. A culture of openness and accountability is essential to prevent such situations or to manage them if they do occur.

In order for us to meet this standard, it is important to learn about potential misconduct and to put a stop to it. Accordingly, it is very important to us to receive information about potential misconduct and to encourage people to report potential misconduct without fear of sanctions or discrimination.

1.2. Contents of the Directive

This guideline answers the following questions:

- How can potential misconduct be reported?
- Is the confidentiality of the identity of the whistleblower guaranteed?
- Who can report potential misconduct?
- What can be reported?
- What happens after a report or how are reports processed?
- How are whistleblowers protected?
- What about data protection?

1.3. To whom does this policy apply?

This policy applies to all employees, trainees, interns, board members, managers, freelancers and other employees (hereinafter uniformly referred to as "employees").

In addition, the policy applies mutatis mutandis to all other persons entitled to report, such as applicants, former employees, all business partners such as suppliers, service providers and customers, shareholders, commercial agents, intermediaries and all other relevant stakeholders who have knowledge of misconduct in the company.

1.4. Primacy of mandatory local law

Mandatory local law is of course not affected by this policy. Where this policy conflicts with mandatory local law, mandatory local law shall prevail.

2. How can potential misconduct be reported?

Internal information: Potential misconduct can be reported internally. It is also possible to simply ask questions or report concerns about the legal compliance or ethical compatibility of certain company activities.

External tips: However, information on potential misconduct can also be provided externally to the competent authorities.

We welcome whistleblowers to report internally first to allow us to investigate and remedy potential misconduct internally, but whistleblowers are not required to report internally first before approaching the relevant authorities with an external report.

2.1. Internal company information

2.1.1. Supervisor/Human Resources

Potential misconduct may be reported to the appropriate supervisor or the human resources department. Whistleblowers may contact the respective representative in person or put the matter in writing. It is possible that a solution can be found quickly and effectively.

2.1.2. CONFDNT whistleblowing system

Whistleblowers can also report potential misconduct through our whistleblowing system. Tips can be given in the following ways:

Online via our website and by telephone via our hotline:

OMG Gruppe:
https://omg.confdnt.com
Tel. DE: +49 8912089251
Tel. EN: +49 8912089268

The website for notices and the hotline for notices are provided by the provider CONFDNT.

The following options can be selected for a notice via the notice web page:

- Anonymous
  No data on the identity of the whistleblower is recorded, but the status of the processing of the whistleblowing can still be tracked anonymously at any time via a QR code or a link. In this way, further additional information on the facts can also be provided anonymously.

- Confidential
  Whistleblowers can provide contact details, e.g. their email address, and are then kept informed about the status of their whistleblowing and whistleblowers in the company can ask questions about the facts, which can simplify and speed up the clarification of the facts.
  In the case of confidential information, the contact details and information on the identity of the whistleblower are processed exclusively by the provider of the whistleblowing system CONFDNT and are not forwarded to the whistleblowers in the company. This is clearly contractually agreed with CONFDNT and CONFDNT is not allowed to forward this information to the company. CONFDNT acts as an anonymisation level between the whistleblowers and the whistleblowers in the company.

- Transparent
  In the case of transparent whistleblowing, the contact data or information on the identity of the whistleblower is passed on by the provider of the whistleblowing system CONFDNT to the whistleblowers in the company and

direct communication can take place between the whistleblowers and the whistleblowers in the company.

2.2. External references to the competent authorities

Whistleblowers can also always contact the competent authorities in case of potential misconduct.

2.3. Anonymous or confidential references

The company will also investigate anonymous tips. However, a proper investigation may be more difficult or impossible in these cases if no further supplementary information on the respective facts can be obtained from the whistleblowers.

The whistleblowing system CONFDNT provides the possibility to give confidential information without revealing the identity of the whistleblowers to the whistleblowers in the company, since the identity of the whistleblowers is only known to the provider of the whistleblowing system CONFDNT and CONFDNT will not and may not reveal the identity of the whistleblowers to the company.

A confidential tip thus combines the advantages of anonymity with the possibility of communication between the whistleblower and the company.

2.4. Telephone advice and personal meeting

Telephone tips or tips given during a personal conversation are recorded with the consent of the person giving the tip or the conversation is recorded. The informants are then provided with the minutes of the conversation for review and correction, and they can confirm the minutes by signing them.

3. Who can report potential misconduct?

All current and former employees of our company, all applicants, business partners such as suppliers, service providers and customers, shareholders, sales representatives, intermediaries and all other relevant stakeholders who have knowledge of misconduct in the company are entitled to report.

4. What can and should be reported?

4.1. All potential grievances

All grievances within the company, all misconduct by employees, all potential violations of applicable law and/or company policies, etc., including the respective suspicion, can and should be reported.

This includes, but is by no means limited to, the following areas in particular:

- Fraud and misconduct in relation to accounting or internal accounting controls
- Corruption, bribery and venality
- Banking and financial crime
- Auditing offences
- Money laundering, financing of terrorist activities,
- Prohibited insider trading
- Infringements of cartel law
- Infringements of competition law
- Violations of data protection law
- Betrayal of secrets, breaches of confidentiality obligations
- Falsification of contracts, reports or records
- Misuse of company assets, theft or embezzlement
- Violations of human rights
- Discrimination against our employees
- Risks to the health and safety of our employees
- Violations of rights of employees or representative bodies
- Environmental hazards

Violations or suspected violations by any employee, including the company's executive bodies and managers, can and should be reported. The same applies if third parties carry out actions that are directed against our company (for example, attempts at bribery by service providers and suppliers).

4.2. Reasonable suspicion

All cases where there is a reasonable suspicion that an incident relevant under this Directive has occurred should be reported.

It will not always be clear to whistleblowers whether a particular action or behaviour constitutes malpractice or a breach of law and/or company policy. Whistleblowers should consider this carefully before whistleblowing. However, it is clearly in the interest of the company to report a suspected case, even if whistleblowers are not 100% sure that it is indeed a case of malpractice that requires company action.

In case of doubt, potential whistleblowers can discuss the case or the suspicion abstractly with a person they trust, e.g. from among their superiors, the human resources department or the works council - if there is one - and agree on whether it is a relevant case that should be reported.

4.3. Concretisation and plausibility / comprehensibility

Each report should be as specific as possible. Whistleblowers should provide as detailed information as possible about the facts to be reported so that the reporting officers can assess the matter properly. In this context, the background, the course of events and the reason for the report as well as names, dates, places and other information should be given. Documents should be provided if available. Personal experiences, possible prejudices or subjective views should be identified as such.
In principle, whistleblowers are not obliged to conduct their own investigations; an exception may apply if they are obliged to do so under their employment contract.

4.4. Good faith or abuse of the whistleblower system

A tip should be made in good faith. If a review of the tip reveals, for example, that there is no reasonable suspicion or that the facts are insufficient to substantiate suspicion, whistleblowers who report a tip in good faith will not be subject to disciplinary action.

The same applies to whistleblowers who deliberately misuse the whistleblowing system to make false reports; they must expect disciplinary measures. Impairment of the whistleblowing system through, for example, manipulation, cover-up or breach of secrecy or confidentiality obligations may also result in disciplinary measures and possibly civil or criminal consequences.

4.5. Obligation to inform

If employees have reason to believe that a matter related to the company constitutes a criminal offence or is likely to cause serious damage to the company or third parties, they have a duty to inform the company. This duty to inform does not apply if the facts are already known to the company or if there is no duty to testify under the Code of Criminal Procedure, e.g. in the case of spouses or relatives under section 52 of the Code of Criminal Procedure.

5. What happens after a report or how are reports processed?

5.1. Acknowledgement of receipt

Whistleblowers will receive an acknowledgement of receipt within seven days of receipt of their whistleblowing, unless the whistleblowing was done anonymously.

When using our whistleblowing system CONFDNT, the confirmation of receipt and the status of processing can also be retrieved for anonymous reports via the QR code or link to the respective report.

5.2. Editing the note

Every report is treated confidentially and in accordance with the applicable data protection laws. Impartial reporting officers who are not bound by instructions are appointed within the company to process the information.

After receipt of a report, the reporting officers acknowledge receipt of the report within 7 days at the latest. The reporting officers carry out an initial check of the plausibility and relevance of the report.

If the reporting officers are of the opinion that further investigations should be carried out, they document this and forward the information to the departments responsible for further investigations within the company. The latter then carry out the internal investigation.

The name of the whistleblower will only be communicated and disclosed within the company if the whistleblower has given his or her express approval.

All employees are obliged to support the authorities responsible for the investigation in their enquiries and to cooperate to the best of their ability in clarifying the suspicion. They are obliged to maintain confidentiality.

The information obtained is documented, with only the necessary data being collected and processed. The investigation will be carried out as quickly as reasonably possible. The unit or units responsible for internal investigations shall keep the reporting officers informed of the progress of the investigations.

The whistleblowers are informed by the reporting officers about the progress of the procedure and receive feedback on the processing status or the measures taken in connection with the whistleblowing within an appropriate time frame, at the latest within three months after receipt of the whistleblowing.

5.3. Conclusion of the investigations and measures

The unit(s) responsible for internal investigations shall inform the respective persons authorised to make decisions after completion of the investigations if a tip-off proves to be accurate and relevant.
Persons authorised to make decisions are persons who have the power to act within the company to remedy, prosecute, punish etc. grievances. As a rule, this will be the management.
The persons authorised to make decisions then decide on the necessary measures in the interest of the company, based on the ascertained facts.

As far as necessary on the basis of the results obtained, the competent authorities are subsequently also involved and the corresponding data are transmitted to them.
If a tip turns out to be false or cannot be sufficiently substantiated with facts, this will be documented accordingly and the procedure will be discontinued immediately. There must be no consequences for the employees concerned; in particular, the case will not be documented in the personnel file.

The Company will also endeavour to use the results and suggestions of any investigation in such a way that misconduct can be corrected in the future, to the extent possible under the existing circumstances.

5.4. Complaint about the way the tip was handled

The company attaches great importance to ensuring that all advice is fully processed and appreciated and that it is always dealt with fairly and appropriately.

If whistleblowers are not satisfied with the way a whistleblower's report has been handled, they can contact a person they trust, e.g. a supervisor, the human resources department, the works council (if there is one) or the management directly.

6. How are whistleblowers protected?

6.1. Confidentiality and secrecy

The protection of whistleblowers is ensured by the confidential treatment of their identity. Confidentiality also applies to all other information from which the identity of the whistleblower can be directly or indirectly deduced.
In principle, the name of the whistleblower will not be disclosed; otherwise, the identity of the whistleblower may be disclosed if the whistleblower consents or if there is a legal obligation to do so.
Whistleblowers shall be informed before their identity is disclosed, unless such information would jeopardise the relevant investigation.
The same applies to confidentiality with regard to whistleblowers as to persons who have assisted in the clarification of a suspicion.

6.2. Protection from reprisals

Any person who gives a tip-off in good faith or cooperates in the clarification of a corresponding suspicion does not have to expect disadvantageous measures and reprisals or the threat or attempt of disadvantageous measures and reprisals as a result of the tip-off or cooperation, whereby this includes in particular the following disadvantageous measures and reprisals:

- Suspension, dismissal or comparable measures
- Downgrading or refusal of a promotion
- Transfer of tasks, change of place of work, reduction in salary, change in working hours
- Refusal to participate in further training measures
- Negative performance appraisal or issuance of a poor employer's reference
- Disciplinary measure, reprimand or other sanction including financial sanctions
- Coercion, intimidation, bullying or exclusion
- Discrimination, disadvantageous or unequal treatment
- Damage (including reputational damage), especially on social media, or causing financial loss (including loss of orders or revenue)
- Early termination or cancellation of a contract for goods or services

- Withdrawal of a licence or permit

This may not apply if the person is involved in the incident to be investigated.
If whistleblowers or persons involved in the investigation of a suspicion believe that they are or have been subject to reprisals as a result, they must report this to their respective superiors or, if the superiors are or were involved in the potential reprisal, to the management.

If there is a presumption that whistleblowers or persons involved in the investigation of the suspicion have suffered reprisals due to the whistleblowing or cooperation, it is up to the person who took the disadvantageous measure to prove that this measure was based on sufficiently justified reasons and does not constitute reprisal due to the whistleblowing or cooperation.

The company will not tolerate any discrimination, harassment or similar treatment of whistleblowers or whistleblowers. The Company will consider the circumstances of each case and may take temporary or permanent measures to protect whistleblowers or cooperators and to protect the interests of the Company.

Any employee or supervisor who dismisses, demotes, harasses, discriminates against or the like any whistleblower or person who cooperates in the investigation of a relevant suspicion on the basis of the whistleblowing or cooperation shall be subject to disciplinary action which, in the most extreme case, may lead to dismissal.

Protection against reprisals also extends to third parties associated with whistleblowers who may suffer reprisals in a professional context, such as other employees or family members of whistleblowers, legal entities owned or worked for by whistleblowers, or with whom whistleblowers are otherwise associated in a professional context.

7. How are reported persons protected?

7.1. Information of the reported person

Any person affected by a tip-off shall be notified of the suspicions directed against him or her at the appropriate time, taking into account the requirements of data protection law, unless such notification would significantly impede the progress of the proceedings to establish the facts. The notification shall be made at the latest after the investigation has been completed.
The notification usually contains the following information:

- the details of the message submitted
- the purposes of the processing
- the legal basis for the processing and the legitimate interests of the company underlying the processing
- the categories of personal data that are processed
- the departments informed of the notification and the persons authorised to access the data
- the recipients or categories of recipients
- The intention to transfer the data to recipients located in an insecure third country and the legal basis for the transfer
- Information on the identity of the whistleblowers or sources, insofar as they have consented to the disclosure of their identity or this is necessary to protect the interests of the persons concerned
- the duration of the storage of the data or the criteria for determining the duration
- the rights of the data subject to information, correction, blocking or deletion or any rights of objection
- Rights of appeal to the supervisory authority

7.2. Right to comment

The person concerned must be heard by the body responsible for internal investigations before conclusions are drawn at the end of the procedure explained above, naming the person. If a hearing is not possible for objective reasons, the competent body shall invite the person concerned to formulate his or her arguments in writing.

7.3. Right to erasure of data

If the suspicion asserted in the notification is not confirmed, the data subject has the right to have his/her data stored by the company in this context deleted.

7.4. Right to complain to the works council

The reported person may exercise his or her right of appeal under sections 84, 85 of the Works Council Constitution Act (BetrVG) and involve the works council.

8. Data protection

8.1. Legal conformity and legal basis

Personal data provided by whistleblowers or collected in the course of internal investigations are processed in compliance with data protection regulations.

The data collected will only be used for the purposes described in this policy. The data is provided in particular to ensure the legal obligations of the company or compliance within the company. The data is processed on the basis of Section 26 (1) of the German Federal Data Protection Act (BDSG) for the fulfilment of contractual obligations or on the basis of the overriding legitimate interests of the company pursuant to Article 6 (1) f) of the German Data Protection Regulation (DSGVO). These legitimate interests are ensuring compliance in the company, in particular the detection and clarification of wrongdoing in the company, behaviour that is harmful to the company, white-collar crime, etc., as well as the protection of employees, business partners, customers and other stakeholders.

8.2. Information and advice

Whistleblowers are provided with the necessary information on data processing and data protection when the data is collected.
All persons whose data are processed by the company within the framework of the procedure (e.g. whistleblowers, reported persons or persons assisting in the clarification) have the right, pursuant to Art. 15 GDPR, to receive information from the company about the data stored by the company about them and further information, such as the processing purposes or the recipients of the data.

8.3. Retention and deletion

Notices will not be retained for longer than is necessary and proportionate to meet the requirements set out in this policy or legal retention periods.
The deletion of the collected data shall generally take place after the conclusion of the internal investigations , at the latest three years after the conclusion of the proceedings. If criminal, disciplinary or civil court proceedings are instituted as a result of misconduct within the meaning of this Directive or abuse of the whistleblowing system, the storage period may be extended until the respective proceedings have been finally concluded.

Personal data that is obviously not relevant for the processing of a specific tip will not be collected or will be deleted immediately if it was collected unintentionally.

8.4. Technical and organisational measures

The data collected and processed as a result of a notice are stored separately from the other data processed in the company. Appropriate authorisation systems and adequate technical and organisational measures ensure that only the persons responsible in each case have access to this data.

8.5. Transfer to third countries

The data is processed exclusively within the EU or the EEA. Only in the case of non-European circumstances may a transfer to unsafe third countries be necessary. In this case, appropriate guarantees are provided in accordance with Art. 46 ff. DSGVO are provided.

8.6. Data subjects' rights

All persons whose data are processed by the company within the scope of the procedure have the right to have their incorrect data corrected, the right to have their data completed, the right to have their data blocked or to have their data deleted, provided that the conditions for this pursuant to Art. 16 et seq. DSGVO are present. A request for deletion is justified, for example, if the data has been processed unlawfully or the data is no longer needed for the purposes for which it was collected.

8.7. Rights of objection

If data are processed on the basis of legitimate interests of the company, the person concerned by such processing may object to the processing of his/her data by the company at any time on grounds relating to his/her particular situation. The company will then either demonstrate overriding legitimate grounds allowing the processing or it will no longer process the data. For the time of this review, the data required for these purposes will be blocked.

8.8. Data Protection Officer

Persons involved in the procedure, including the whistleblowers themselves, can contact the company's data protection officer at any time to have it checked whether the rights existing on the basis of the relevant applicable provisions have been observed.

8.9. Right of appeal to the data protection supervisory authority

If data subjects believe that the company is not processing the data in accordance with applicable data protection law, they may lodge a complaint with the competent data protection supervisory authority.

9. Consequences in the event of infringements

A violation of this policy may result in measures under labour law, including termination of employment without notice or, in the case of freelancers, termination of the cooperation without notice. Criminal sanctions and civil law consequences such as compensation for damages are also possible.