WHISTLE-BLOWER POLICY

MYTY

Contents

1. Scope and applicability **4**

2. Purpose **4**

3. Definitions and terminology **5**

4. Disclosure procedure **6**

4.1. Requirements for disclosure 6

4.2. Procedural rules 7

4.2.1. Internal disclosures 8

4.2.2. Disclosure via the whistleblower portal 8

5. Procedure following a disclosure **9**

5.1. Receipt of a disclosure 9

5.2. Documenting the disclosure 9

5.3. Conducting an investigation 10

6. Protection of whistleblowers and persons involved in the investigation **10**

6.1. Confidentiality and secrecy 10

6.2. Protection from sanctions 11

7. Protection of reported persons **11**

8. Abuse of the whistleblower system **12**

9. Further rights of data subjects **13**

10. Right to lodge a complaint **14**

Version 1.0 of 04.10.2023

11. Implementation, responsibility 14

12. Data protection 15

1. Scope and applicability

The aim of this policy is to generate trust and encourage participation by employees, management, business partners, customers, suppliers, etc. of the MYTY Group.

This policy regulates the setting up and use of a whistleblower system. It indicates when and how potential cases of wrongdoing are to be disclosed. The policy also explains how to deal with such disclosures. It should be noted at this point that any whistleblowers need not fear sanctions against them as a result of submitting a disclosure in good faith. Whistleblowers are also guaranteed maximum confidentiality.

Where stricter rules, statutory regulations, etc. apply to individual functional areas, those stricter regulations take precedence over the terms of this policy.

2. Purpose

The aim of this policy is to operate a whistleblower system for disclosing and resolving corporate misconduct, conduct that is damaging to the company, white-collar crime (etc.) and protecting all employees, business partners, customers, etc. The following rules are intended to support both employees and company management in detecting, disclosing and eliminating any potential wrongdoing.

Illegal, immoral or illicit conduct in the workplace which employees are unable to resolve themselves is to be disclosed to a contact person designated by the company. The whistleblower system, however, is not intended for submitting general complaints about other employees.

3. Definitions and terminology

Persons authorised to submit a disclosure

All current employees and managers of the MYTY Group, as well as third parties, are authorised to make disclosures.

Potentially affected persons

All employees, managers, etc. suspected of having been involved in a reportable incident can be reported. The same applies if a third party commits an act directed against one or more companies.

Object of the disclosure

Any disclosure of misconduct must, in principle, be limited to conduct that is in conflict with the company's interests and concerns a criminal offence or a serious misdemeanour. This applies in particular to offences such as corruption, fraud, prohibited insider trading and conduct that violates human rights.

Duty to disclose

There is a duty to disclose in all cases where employees have reason to believe that a specific situation:

- constitutes a criminal offence or
- may cause serious damage to the company or a third party; and
- is directly attributable to a company of the MYTY Group.

The duty to disclose does not apply if the situation is already known to the authorised decision-makers within the company in a way that is evident to the employee or where criminal procedures would permit the right of refusal to testify (e.g. if employees would

incriminate themselves or their spouse).

4. Disclosure procedure

All persons authorised to submit a disclosure are encouraged to openly and directly disclose reports, misconduct, hazards, etc. which are known to them in accordance with this policy, stating their contact details where possible. In cases where it would appear unreasonable to expect whistleblowers to make a disclosure which could be attributed to them, they may also make a disclosure anonymously.

4.1. Requirements for disclosure

"Good faith"

Disclosures should only be submitted where all whistleblowers are reporting in good faith that the facts they disclose are accurate and true. They are not reporting in good faith if it is known that a disclosed fact is untrue. In the event of doubt, the situation in question should not be portrayed as a fact, but as a suspicion or assessment, or a statement by another person. A disclosure should point out any potential doubts. That said, it is preferable to report any suspicions in good faith than not to disclose them.

Reasonable belief

Whistleblowers should only disclose cases where reasonable grounds exist to believe that a process relevant to this policy has taken place. It will not always be clear to whistleblowers whether a particular act or conduct must be reported in accordance with the principles of this policy. Whistleblowers should check this carefully prior to making a disclosure. In the event of doubt, employees should disclose suspicions in good faith rather than failing to disclose them.

Specific and coherent

Every disclosure should be as specific as possible. Whistleblowers should provide the most detailed information possible about the circumstances to be disclosed so that the matter can be properly assessed.

A disclosure must contain at least the following information:

- Reason for disclosure;
- Background and sequence of events;
- Names of the persons involved;
- Place and date of the sequence of events;
- If available: documents, evidence.

Personal experiences, possible prejudices or subjective opinions must be identified as such.

Whistleblowers are, in principle, not required to conduct their own investigations. Exceptions may apply as a result of provisions in the employment contract.

4.2. Procedural rules

Whistleblowers have various options available for submitting a disclosure effectively and reliably. In particular, the disclosure can be communicated internally in the respective company or via the MYTY Group's whistleblower portal. The involvement of other external third parties, such as the police, should only take place in exceptional cases and after consultation with the contact person previously contacted. The reporting procedure described below should be used appropriately in accordance with the reporting levels described, taking into account the personal and affected interests of the persons involved and of the company.

4.2.1. Internal disclosures

Line manager

The first point of contact should always be the line manager or the employee directly responsible for the subject matter. This is usually the easiest way to address a problem from the working environment, to resolve any misunderstandings and ensure a good and open working atmosphere. If the matter is justified, the contact person will initiate further steps.

Management

If, for factual or personal reasons, it appears necessary to make the disclosure directly to the management, the whistleblowers may also contact the latter directly. This applies in particular if, in the view of the employee, the disclosure could not be followed up in the proper way by the line manager, the persons responsible for the matter or the contact person in the relevant department. Direct communication with the management is particularly necessary if it is to be feared that line managers, persons responsible for the matter or contact persons in the relevant department are involved in the matter or if whistleblowers have reason to fear serious personal discrimination.

Compliance Officer

If, for factual or personal reasons, it appears unreasonable or impractical for whistleblowers to disclose to line managers or management, the whistleblower can also contact the MYTY Group Compliance Officer directly (neutral contact person in the Group without an executive function) via the whistleblower portal (see 4.2.2.).

4.2.2. Disclosure via the whistleblower portal

Whistleblowers also have the option of using the whistleblower portal of the MYTY Group to disclose wrongdoing or a problem. A disclosure via the whistleblower portal

should only be made if internal communication appears unreasonable or if whistleblowers assume that their disclosure will not be handled internally in the proper manner. Anonymous disclosures can also be made via the whistleblower portal.

The MYTY Group's whistleblower portal can be accessed at myty.hintbox.eu.

5. Procedure following a disclosure

5.1. Receipt of a disclosure

Every disclosure will be processed confidentially and taking into account current data protection laws.

Once a disclosure has been received, the receiving office will carry out an initial review of the disclosure, in particular regarding whether there is evidence to confirm or refute the information provided.

If the receiving office is of the opinion that further investigations are required, it documents this and then initiates the internal investigations.

5.2. Documenting the disclosure

The information obtained is documented, although only the necessary data is collected and processed. If the findings obtained render it necessary, then other relevant bodies, authorised decision-makers and then, if necessary, the authorities are involved, and the corresponding data is forwarded to them.

5.3. Conducting an investigation

The investigation will be completed as quickly as possible within the appropriate scope. The whistleblower will be informed, if requested and where possible, of the progress of the procedure by the office responsible for the investigation.

If a disclosure turns out to be false or cannot be sufficiently substantiated by fact, this is documented accordingly and the procedure is terminated with immediate effect. There must be no consequences for the employees concerned; in particular, the course of events must not be documented in the personnel file.

The results and recommendations from each investigation should be used to prevent possible misconduct and eradicate this in the future.

6. Protection of whistleblowers and persons involved in the investigation

6.1. Confidentiality and secrecy

The identities of the whistleblowers and the persons involved in the investigation are treated as strictly confidential.

If whistleblowers provide their contact details, these will be stored and used whilst taking into account data protection regulations. When data is collected, they will be informed of both the purposes of data storage and use of the data. The same applies if the personal data is to be transferred to other bodies.

The name of the whistleblower will only be made known if this has been expressly

authorised or if there is a corresponding legal obligation to do so. This applies in particular if disclosure is essential to enable the persons affected by the report to exercise their right to a hearing.

The whistleblowers are always informed before their identity is revealed.

6.2. Protection from sanctions

Any person who makes a disclosure in good faith or is involved in the investigation of suspected wrongdoing must be sure that they will not experience any negative consequences as a result of the disclosure or their involvement (e.g. demotion or dismissal). This may not apply if the person is implicated in the event to be resolved.

If the whistleblower or a person involved in resolving a case of suspected wrongdoing is of the opinion that disadvantage, discrimination, harassment or similar has occurred as a result, this must be reported in accordance with section 4. via the reporting channels provided there. Disadvantaging, discrimination, harassment or similar of whistleblowers or any other person involved will not be tolerated.

Any employee or line manager who, based on the disclosure or involvement, dismisses, degrades, insults or discriminates against a whistleblower or a person involved in investigating a case of suspected wrongdoing must expect disciplinary action, which in extreme cases may lead to dismissal.

7. Protection of reported persons

Any person who is the subject of a disclosure will be notified within one month and in accordance with data protection regulations of the allegations made against them, unless such notification would significantly impede the ongoing process of establishing

the facts. Notification will be provided no later than upon completion of the investigations.

The person concerned must be heard by the competent body or the authorised decision-makers before conclusions are drawn naming the person. If a hearing is not possible for objective reasons, the competent body or the authorised decision-makers will ask the person concerned to provide their arguments in writing. The authorised decision-makers then decide on the measures required in the interests of the company.

If the case of suspected wrongdoing asserted in the report is not confirmed, the person concerned has a right to erasure of their data stored by the company in this context.

8. Abuse of the whistleblower system

All employees are asked to disclose wrongdoing, misconduct, etc. Whistleblowers must ensure that the facts are presented objectively, accurately and comprehensively. Personal experiences, potential prejudices or subjective opinions must be identified as such.

A disclosure must be made in good faith. If the review of the disclosure reveals that there is no reasonable suspicion or that the facts are not sufficient to substantiate suspicion, whistleblowers who submit a disclosure in good faith will not be subject to disciplinary action.

Whistleblowers who deliberately abuse the whistleblowing system to make false disclosures must expect disciplinary action. Compromising of the whistleblowing system (e.g. through manipulation, cover-up or collusion) may also result in disciplinary

action.

Measures that can be taken include warnings or dismissals. In addition, abuse of the whistleblower system can also have consequences under civil or criminal law.

9. Further rights of data subjects

All persons whose data is processed as part of the procedure (e.g. whistleblowers, reported persons or persons involved in resolving the problem) have the right of access to any stored personal data or information concerning them in accordance with Art. 15 GDPR.

All persons whose data is processed by the company as part of the procedure (e.g. whistleblowers, reported persons or persons involved in resolving the problem) have the right to rectification of inaccurate data concerning them, the right to have incomplete data completed and the right to block their data or have it erased, provided that the requirements of Art. 16 et seq. GDPR are met. A request for erasure is justified, for example, if the data has been processed unlawfully or if the data is no longer necessary in relation to the purposes for which it was collected.

If the data has been transferred to a third party, the data recipient of the data will be notified of the rectification, erasure or blocking of the data in accordance with the statutory regulations.

If data is processed on the basis of the company's legitimate interests, the data subject affected by this processing can object 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 that there are overriding legitimate grounds for the processing or it may no

longer process the data.

10. Right to lodge a complaint

Both the whistleblowers and the reported persons can contact their direct line manager, management or People & Culture if they have any information regarding a breach of this policy.

Both the whistleblowers and the reported persons can contact the contact persons named in Section 11 if they consider the investigations carried out to be incorrect or inadequate or if they believe that they have been unfairly disadvantaged in the course of the investigations. In this case, the measures necessary for reviewing the matter will be initiated and the complainant will be informed accordingly.

11. Implementation, responsibility

The respective management is responsible for publication and implementation of this policy. This also includes creating conditions in all MYTY Group companies which enable whistleblowers to report in confidence. The following measures are to be implemented:

- Informing of all employees regarding the whistleblower system
- Appointment of one or more local contact persons within the company
- Informing and training of the contact persons and the management regarding the correct implementation of the procedure and implementation of policy requirements.

The management monitors the implementation of the policy. Among other things, it shall review the effectiveness of measures taken in response to a suspicion raised in

accordance with this policy. The management may appoint bodies within the company to support it in monitoring.

12. Data protection

Personal data is collected and stored as part of the procedure. This data is handled in compliance with the applicable data protection laws, in particular the GDPR. Only the data which is objectively necessary for the purposes of this policy is collected and processed.

The data collected as a result of a report is stored separately from other data stored in the company. Appropriate technical and organisational measures ensure that only the responsible persons in each case have access to this data. This also applies to the whistleblower's data.

Data collected in connection with a disclosure which is not relevant to the procedure will be deleted immediately. Otherwise, the data collected will generally be deleted within two months of the conclusion of the company's internal investigations. If criminal, disciplinary or civil court proceedings are initiated as a result of misconduct within the meaning of this policy or of abuse of the whistleblower system, the storage period may be extended until the respective proceedings have been legally concluded.

Persons involved in the procedure, including the whistleblower themselves, can contact the company's data protection officer at any time to check whether the rights existing under the relevant applicable provisions have been observed. If a data subject is of the opinion that the company is not processing the data in line with the applicable data protection law, they can lodge a complaint with the data protection supervisory authority.