PLANATOL®
smart gluing

Dated 01.05.2021

Whistleblower System Directive

Setting up and using a whistleblower system within the Planatol Group

Table of Contents

1. Scope

a. The aim of this Directive is to create trust and to encourage the employees, management, business partners, customers, suppliers, etc. of the Planatol Group (Planatol GmbH and Planatol System GmbH) to participate.

b. This Directive regulates the establishment and use of a whistleblower system. It indicates when and how potential cases of wrongdoing are to be disclosed. In addition, the Directive explains how to handle such disclosures. At this point, the reader should take note that whistleblowers will not have to fear sanctions against them as a result of submitting a disclosure in good faith. Whistleblowers are also accorded maximum confidentiality.

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

d. This Directive supplements and adds further detail to the whistleblower system described in the Code of Conduct.

2. Pronouns

For reasons of better readability, masculine pronouns will be used in this text. Please note that the sole use of masculine pronouns should be regarded as gender-unspecific. This is in no way intended as gender discrimination or violation of the equality principle.

3. Objectives

The aim of this Directive is to set up a whistleblower system for disclosing and resolving corporate misconduct, behaviour that damages the image of the company, business crimes (among other things) and protecting all employees, business partners, customers, etc. The following rules are aimed at helping both the employees and the company's management detect, disclose and eliminate any potential wrongdoing.

Illegal, immoral or illicit conduct in the workplace that employees are unable to resolve themselves is to be disclosed to a contact person designated by the company.

The whistleblower system is not, however, to be used to voice general grievances about other employees.

4. Definitions and terminology

a. **Persons authorised to submit a disclosure**
All current employees and managers of the Planatol Group and third parties are entitled to make disclosures.

b. **Potentially affected persons**
All employees, managers, etc. suspected of being involved in a reportable event may be reported. The same applies when a third party commits an act aimed to harm one or several companies.

c. **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 is particularly true for violations of the Code of Conduct or offences such as corruption, fraud, prohibited insider trading and conduct in breach of human rights.

d. **Duty to disclose**
It is always mandatory to submit a disclosure when an employee has reason to assume that a certain situation:

- constitutes a criminal offence or
- may lead to serious damage to the company or to third parties; and
- can be directly attributed to a company of the Planatol Group.

Reporting is not mandatory if the situation is already known to the decision-makers within the company in a way that is evident to the employee or where criminal procedures permit the right of refusal to testify (e.g. if employees would incriminate themselves or their spouse).

5. Disclosure procedure

All persons entitled to make a disclosure are encouraged to disclose any reports, misconduct, hazards, etc. openly and directly in keeping with this Directive, if possible citing their contact data. In cases in which it appears unreasonable to expect whistleblowers to make a disclosure which could be attributed to them, they may also submit an anonymous disclosure.

5.1. Requirements for disclosure

a. **"Good faith"**
Disclosures should only be made if the whistleblower believes in **good faith** that the facts he is disclosing are accurate and true. He is not reporting in good faith if he is aware 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. At the same time, it is better to voice any suspicions in good faith than not to disclose them.

b. **Reasonable belief**
The whistleblower should only disclose cases in which he has **reasonable grounds to believe** that a process relevant to this Directive is taking place. It will not always be obvious to the whistleblower whether a certain action or behaviour is to be disclosed in accordance with the principles of this

Directive. The whistleblower should carefully check this before making his disclosure. In the event of doubt, the employee should disclose his suspicions in good faith rather than failing to disclose them.

c. **Specific and conclusive**
Any disclosure should be as specific as possible. The whistleblower should provide the recipient with the most detailed information possible about the situation to be disclosed, so that the latter can assess the matter correctly.

d. A disclosure must contain at least the following information:

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

e. Personal experiences, potential biases or subjective opinions are to be indicated as such.

f. The whistleblower is in principle not obliged to conduct his own investigations. There may be exceptions to this, as set out in the employment contract.

5.2. Procedural rules

Whistleblowers have several options for the effective and reliable submission of a disclosure. In particular, the disclosure may be communicated internally within the relevant company (see Section a.) or via the Blue Cap AG "Whistleblower Hotline" (see Section b.). Any involvement of other external third parties, such as the police, should only be brought about in exceptional cases and following a prior consultation with the designated contact person.

Taking into account the personal and affected interests of the persons involved and the company, the reporting procedure described below should be used to the appropriate degree.

a. **Internal disclosures**

(a) Line manager
The first person contacted should always be the line manager or the person who is directly responsible for such matters. This is usually the easiest way to address a problem in the work environment, to clear up misunderstandings and to ensure a good and open work atmosphere. If the matter is justified, the contact person will initiate further steps.

(b) Management
If it appears necessary for factual or personal reasons to make the disclosure directly to the management, the whistleblower may also contact the latter directly. This particularly applies when – in the opinion of the employee – the disclosure could not be properly followed up by the line manager, the person responsible for such matters or the contact person in the relevant department.

Direct communication with the management is especially required if there are fears that the line manager, the person responsible for such matters or the contact person in the relevant department is involved in the situation or when the whistleblower has reason to fear serious personal discrimination.

(c) Compliance Officer

Where it appears unreasonable or impractical for factual or personal reasons that the disclosure should be submitted to the line manager or to the management, the whistleblower may also approach the Compliance Officer of the Planatol Group directly.

Contact person: Mr. Michael Steinke, compliance@planatol.de, 08031/720-114

b. Disclosure via the Blue Cap AG Whistleblower Hotline

A person submitting a disclosure also has the option of using the Blue Cap AG Whistleblower Hotline in order to disclose misconduct or a problem. A disclosure to the Whistleblower Hotline should only be made when internal communication appears unreasonable or when whistleblowers believe their disclosure will not be properly processed internally.

Persons making a disclosure have the option of contacting the Whistleblower Hotline by phone or e-mail to submit their disclosure.

The Whistleblower Hotline may be accessed as follows:

- compliance@blue-cap.de
- +49 (0) 89 / 288 90 907

6. Procedure following a disclosure

6.1. Accepting the disclosure

a. Every disclosure will be processed confidentially and taking into account current data protection laws. The whistleblower will receive an acknowledgement of receipt within a period of 7 days, provided that he has waived his anonymity.

b. Once a disclosure has been received, the receiving department will conduct an initial review of the disclosure, especially noting whether there is any evidence that would confirm or refute the information transmitted.

c. If the receiving department is of the opinion that there should be further investigation, this will be documented and the information will be forwarded to the company's responsible department. This department will then conduct the internal investigations.

d. If the report was received via the Blue Cap AG Whistleblower Hotline, and where the latter is of the opinion that further investigation is to take place, it will document this and inform the whistleblower (if he is not anonymous). The information will also be forwarded to the relevant department of the company, which will then conduct the internal investigations. Any forwarding of the information to the company by Blue Cap AG will only take place at the time and to the extent that the whistleblower has authorised Blue Cap AG to do this by waiving his or her duty of confidentiality in this regard. The company will only be informed about the name of the whistleblower if the latter has granted prior permission to do so.

6.2. Documenting the disclosure

The information that is gathered is documented, with only the required data being collected and processed. Where required on the basis of the findings, the other relevant departments, decision-makers and then, if necessary, the authorities will be contacted and the corresponding data forwarded to them.

6.3. Conducting an investigation

a. The investigation is to be carried out as quickly as possible within the appropriate scope. On request and insofar as this is possible, the whistleblower will be kept informed about the progress of the proceedings by the department responsible for the investigation. This information must be received before expiry of a period of 3 months following confirmation of receipt of the disclosure by the relevant department, provided that the whistleblower has waived his anonymity.

b. If a disclosure turns out to be incorrect or cannot be backed up by sufficient facts, this will be documented correspondingly and proceedings terminated with immediate effect. The employee that is the subject of the disclosure shall not suffer any negative consequences; in particular, the procedure will not be documented in his personnel file.

c. The results and recommendations of each investigation should be used in such a way as to prevent misconduct and to eradicate it in the future.

7. Protecting the whistleblower and the person involved in investigating the case

7.1. Confidentiality and secrecy

a. The identities of the whistleblower and the persons involved in resolving the case will be kept strictly confidential.

b. If the whistleblower provides his contact data, these are stored and used taking data protection regulations into account. When his data are collected, he shall be informed of the purpose for which the data is being stored and used. The same applies when his data are forwarded to other units.

c. The name of whistleblower shall only be made known if he has specifically authorised this to take place or where there is a corresponding legal obligation. This applies, among other things, if the name must be made known for the persons that are the subject of the whistleblowing to make use of their right of consultation.

d. Whistleblowers must always be informed before their identity is revealed.

e. The provisions of Sections b. to d. also apply to persons who have participated in the resolution of suspicions.

7.2. Protection against sanctions

a. All persons who make a disclosure in good faith or are involved in resolving a corresponding suspicion 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 involved in the incident to be resolved.

b. If whistleblowers or people involved in the investigation of a suspicion believe that they have been disadvantaged, discriminated against, harassed or similar, they must disclose this to their line manager. Alternatively, such an incident may be disclosed in line with Clause 5 using the reporting channels provided there. Discrimination, harassment or similar treatment of the whistleblower or a contributor will not be tolerated. The company concerned will examine the circumstances of each case and may take temporary or permanent measures to protect the whistleblower or the person involved and to safeguard the interests of the company. The company shall inform the persons concerned in writing about the result of the respective investigation.

c. Any employee or line manager who, because of a disclosure or cooperation in the investigation into a suspicion, dismisses, demotes, insults, discriminates against or similarly treats a whistleblower or a person cooperating, shall be subject to disciplinary action, which in the most extreme case may lead to dismissal.

8. Protecting the reported person

a. Any person that is the subject of a disclosure shall be notified of the suspicions directed against him within one month, taking into account the requirements of data protection laws, unless such notification would significantly impede the progress of the procedure used to establish facts. The notification shall be submitted at the latest once the investigation has been completed.

b. The person concerned shall be heard by the competent body or persons authorised to take decisions, before conclusions are drawn that name the person. If a hearing is not possible for objective reasons, the competent body or persons authorised to make decisions will request the person concerned to forward his arguments in writing. Thereafter, the persons authorised to take decisions shall decide on the measures necessary in the interests of the company. The person concerned is entitled to call upon a member of the works council to be present at the hearing.

c. If the suspicion raised in the disclosure is not confirmed, the person concerned has the right to have his data deleted that was stored by the company in this context.

9. Abuse of the whistleblower system

a. Every employee is called upon to disclose wrongdoing, misconduct, etc. However, whistleblowers must ensure that they present the facts objectively, accurately and comprehensively. Personal experiences, potential biases or subjective opinions are to be identified as such.

b. A disclosure must be made in good faith. If the review of the whistleblower's disclosure indicates that there is no reasonable suspicion or that the facts are insufficient to substantiate suspicion, whistleblowers who file a disclosure in good faith need not fear disciplinary action.

c. Whistleblowers who deliberately misuse the whistleblowing system to make false disclosures can expect disciplinary action. Interference with the whistleblowing system (e.g by manipulation, co-ver-ups or collusion) may also result in disciplinary action.

d. Possible actions include warnings or dismissals. Misuse of the whistleblowing system may also have consequences under civil or criminal law.

10. Other rights of data subjects

a. Any person whose data are being processed by the company as part of the procedure (e.g. the whistleblower, the reported person or persons involved in resolving the problem) shall have the right of access to any stored personal data or information concerning him as per Art. 15 GDPR. They will receive the information on request from the Compliance Officer (for contact data, see Section 5.2 a. (c)).

b. Any person whose data are processed by the company as part of the procedure (e.g. the whistleblower, the reported person or persons involved in resolving the problem) shall have the right to the rectification of incorrect personal data, the right to have incomplete data completed and the right to block their data or have it erased, as long as the requirements as per Art. 16 et seq. GDPR have been met. For example, a request for erasure is justified if the data were unlawfully processed, or are no longer required for the purposes for which they were collected. This applies, among other things, in the case shown in Section 10.c. of the Directive.

c. If the company has forwarded the data to a third party, it will notify the recipient of the data of the rectification, erasure or blocking of the data in accordance with the legal regulations.

d. If data are processed on the basis of the legitimate interests of the company, data subjects can always object to the processing of their data on grounds relating to their particular situation. The company will then either demonstrate compelling legitimate grounds for processing the data, or will not be allowed to process the data.

11. Right to lodge a complaint

a. The whistleblower and the reported person may contact their line manager, the management or the Blue Cap AG Whistleblower Hotline regarding any information about a breach of this Directive.

b. The whistleblower and the reported person may contact the contact person listed in Section 11.a. if they believe that the investigation is incorrect or inadequate, or if they feel that they are being unjustifiably disadvantaged in the investigation. In this case, the required measures to review the issue shall be initiated and the complainant correspondingly informed.

c. The reported person can make use of his right to make complaints and, if the company has a works council, call on a member of the works council for assistance in accordance with Sections 84, 85 BetrVG (German Works Constitution Act).

12. Implementation, responsibility

a. The respective management is responsible for announcing and implementing this Directive. This also includes creating conditions at all Planatol Group companies that make it possible for whistleblowers to submit disclosures in a spirit of trust.

To do this, the following measures need to be implemented:

- Informing and educating all employees about the whistleblowing system.
- Assigning one or more local contact persons within the company.
- Informing and training the contact person and management in the correct handling of the procedure and the implementation of the requirements of the Directive.

b. The management shall check the implementation of the Directive. Among other things, it shall review the efficiency of measures taken in response to a suspicion voiced in accordance with this Directive. The management may appoint bodies within the company that support them in this endeavour.

13. Information, training, contact persons

a. The Directive is available to all employees on the Intranet. Employees who do not have access to the Intranet will receive a printed copy. Alternatively, this can be requested at any time from the personnel office.

b. All employees are obliged to complete the company-provided training on the subject of whistleblowing.

c. In the event of any questions, suggestions, etc., regarding the regulations of this Directive, please contact the Compliance Officer or the management of your company.

14. Data protection

a. Personal data are collected and stored as part of this procedure. These data will be handled in accordance with current data protection laws, including but not limited to the GDPR. Only data that are objectively required for the purposes of this Directive will be collected and processed.

b. The data collected as the result of a disclosure will be stored separately from other data stored by the company. Appropriate technical and organisational measures are taken to ensure that only the persons responsible have access to these data. This also applies to the whistleblower's data.

c. Any data collected in connection with a disclosure that are not relevant for the procedure will be deleted immediately. In all other cases, the data collected will be deleted within two months after completion of the company's in-house investigations. If misconduct according to this Directive or an abuse of the whistleblower system should lead to criminal, disciplinary or civil court proceedings, the storage period may be extended until the court has taken a decision in the proceedings in question.

d. Persons involved in the proceedings, including the whistleblowers themselves, may approach the data protection officer of the company at any time to find out whether existing rights have been taken into account, based on the relevant and applicable regulations. Where a data subject is of the opinion that the company is not processing the data in line with current data protection laws, a complaint may be filed with the data protection supervisory authority.

Data protection officer:
Consulting-L, Stefan Leißl, Sanderstraße 47, 86161 Augsburg
leissl@consulting-l.de
0821 / 6508 8580