Whistleblowing policy

Introduction

In accordance with the Belgian Act of 28 November 2022 on the protection of whistleblowers of breaches of Union or national law established within a legal entity in the private sector (hereinafter referred to as "the Whistleblower Act"), employers with at least 50 employees have the obligation to create and introduce a whistleblowing policy.

The Whistleblower Act applies to any person who obtains information, within a work-related context, about a violation of legal or regulatory provisions or directly applicable European provisions. This concerns, employees, agency workers, trainees, former employees, applicants, etc.

Whistleblowing policy

General provisions

Our company acknowledges the importance of a whistleblowing policy for good corporate governance and responsible entrepreneurship.

Our whistleblowing policy describes the manner in which our organisation deals with reports of a suspected violation.

For which violations?

The concept of violation can be defined as acts or omissions that are contrary to legislation relating to

- public procurement contracts
- financial services products and markets, prevention of money-laundering and the financing of terrorism,
- product safety and conformity,
- transport safety,
- environmental protection,
- radiation protection and nuclear safety,
- safety of food and animal feed, health and well-being,
- public health,
- consumer protection,
- protection of privacy and personal data and security of network and information systems,
- combatting tax fraud,
- combatting social security fraud, and
- the rules on the functioning of the European internal market (competition and State aid).

In accordance with this whistleblowing policy, information, including reasonable suspicions, about actual or potential violations that have occurred or are highly likely to occur, as well as

about attempts to conceal such violations, can be reported. The basic principle in this respect is that the suspicion of a violation is based on reasonable grounds.

Reporting a violation

It is advisable to first report a (suspected) violation to the immediate supervisor/manager.

If the whistleblower feels that they cannot raise their concerns with these persons for any reason whatsoever, they can file an internal report via the internal reporting channel. The procedure to be followed is described below.

It is highly recommended that violations be reported via the internal procedure. Internal reporting is the most efficient way to enable the company to investigate the matter in depth and to take appropriate measures to deal with a violation.

However, the possibility also exists to report a violation, either after first having reported it internally or immediately, to a locally competent authority within the specific area of responsibility, e.g. to the Federal Public Service for Finance, the Federal Public Service for Employment, Labour and Social Dialogue, the National Office for Social Security, the Financial Service and Markets Authority, the National Bank of Belgium, the Federal Agency for the Safety of the Food Chain, the Federal Agency for Nuclear Control, the Data Protection Authority, the Federal Ombudsman etc. (external reporting).

Public reporting or disclosure of information about violations is possible if the following strict conditions are met:

1. The whistleblower first made an internal or external reporting but no appropriate measures have been taken, and
2. The whistleblower has reasonable grounds to believe that:
    - the violation may constitute an imminent or real danger to the public interest; or
    - in case of external reporting, there is a risk of retaliation or it is not likely that the violation will be remedied efficiently due to the specific circumstances, e.g. because evidence may be concealed or destroyed or a public authority may be in league with the author of the violation or be involved in the violation.

Internal reporting

Internal reporting procedure

Initially, the violation must be reported to the contact person within our company, Sonja Gelderblom, +31320229602, PZ@detraay.com.

If the suspected violation concerns this contact person, it can be reported to the management.

A report must be sufficiently detailed and documented and contain at least the following information, if available:

- The name and contact details of the whistleblower;
- A detailed description of the events;
- The date and place on which the events took place;

- The name of the persons concerned or other information that makes it possible to identify them;
- The names of any persons who may confirm the reported facts;
- Any other information or elements that may be helpful for the verification of the facts.

The contact person is responsible for taking receipt of a report and will also take up the responsibilities of a report manager (see also below).

Oral reporting is possible by phone or voice message.

The reporting preferably takes place in the form of a personal conversation, but is evidently also possible in writing.

At the whistleblower's request, a reporting can also be made during a face-to-face meeting within a reasonable period of time.

The contact person will always propose a personal conversation on the basis of a written report.

Subsequent procedure

The whistleblower will receive an acknowledgement of receipt of the report at the latest seven days following that receipt.

The report manager will investigate the report promptly and in depth, taking into account the principles of confidentiality, impartiality and fairness with regard to all persons concerned. The report manager can contact the whistleblower in order to obtain more information and/or evidence with regard to the violation. If necessary for the investigation, an investigation team may be set up, consisting of e.g. external service providers, advisors, experts etc.

The report manager will maintain contact with the whistleblower, requesting more detailed information of necessary and providing feedback.

At the latest three months following the acknowledgement of receipt of the report, feedback will be provided to the whistleblower as to the on-going or completed investigation.

Upon completion of the investigation, the report manager will draw up a report relating to the investigative measures taken and their outcome.

This report can be shared outside the investigation team, exclusively on a need-to-know basis, with the management in order to take a final decision as to whether or not the violation is proven and in order to determine the appropriate measures that are needed to put an end to the violation and safeguard the company's interests.

The report manager will draw up a final report containing a description of the facts and the final decision:

- If the violation is proven, the final report contains the measures that will be taken to put an end to the violation;

- If the investigation reveals that no or insufficient proof of the violation is available, no further action will be undertaken.

The report manager will inform the whistleblower of the outcome of the investigation and of the decision that has been taken.

Guarantees for the whistleblower

Whistleblowers enjoy protection if they have reasonable grounds to believe that the reported information about violations was accurate at the time of the reporting and that this information falls within the scope of application of this whistleblowing policy. The whistleblower will not lose the benefit of protection on the sole ground that the reporting made in good faith is revealed to be inaccurate or unfounded.

The contact person/report manager will not disclose the identity of the whistleblower.

The contact person/report manager can only disclose the identity of the whistleblower:

- if the whistleblower grants explicit (written) permission to do so of their own free will; or
- if the whistleblower deliberately breaches the obligation of confidentiality.

The confidentiality of the whistleblower's identity will not apply if disclosure is required by binding legislation within the context of investigations by national authorities or of legal proceedings. The competent authorities will inform the whistleblower in advance of the reasons for the disclosure, unless this would jeopardise the investigations or legal proceedings.

Any form of retaliation, including threats of and attempts at retaliation, is prohibited.

Whistleblowers acting in accordance with this policy can report (suspected) violations without jeopardising their contractual position or having to fear any other negative consequences. This implies that their position in the company will not in any way be impacted as a result of their question or reporting, provided that they act in good faith.

The company assumes that whistleblowers will report (suspected) violations in good faith. If upon closer investigation, the report manager does not find any corroboration of specific reported facts or if the suspicions appear to be unfounded, no measures will be taken against whistleblowers who expressed their concerns in good faith. However, the company cannot allow whistleblowers to deliberately report suspicions of which they know or are deemed to know that they are untrue. Appropriate penalties will be imposed in case of deliberately false reports. Anyone who reports a (suspected) violation in bad faith may be held liable for the damage incurred as a result of a false report. Anyone who deliberately reported or disclosed false information may be prosecuted for defamation.

Processing of personal data and your rights

Meli nv is the data controller for the personal data that are processed within the context of an internal reporting. This implies that both the whistleblower and the person concerned can address the company in order to exercise their right of information, access, rectification and erasure, taking into account the following restrictions:

- The person concerned (to whom the reported violation relates) has no right of access to the identity of the whistleblower or of third parties (nor to any elements that may make their identification possible), unless the latter have given their consent or in case of a false report or defamatory allegations by the whistleblower or false statements by a third party;
- The whistleblower has no right of access to the personal data of the accused nor to those of any third party, unless the investigation reveals that the accused wrongfully discredited the whistleblower (e.g. by stating that the whistleblower was involved themselves in the malpractices they reported) or third parties acted in bad faith (e.g. false witness statements).
- The personal data of the parties involved are not deleted as long as the internal and/or external (police/judicial/administrative) investigation is ongoing.

In addition to the facts, the names, positions and contact details of the whistleblower and of the accused will be processed during the reporting procedure. The processing of these personal data is necessary within the context of the Whistleblower Act.

The personal data will be processed with a view to the processing, investigation and follow-up of the report. The processing of these personal data for these purposes is based on our legitimate interest and our legal obligation to process the above-mentioned personal data. Your personal data will only be shared with the persons who need them in order to achieve these purposes.

The transfer of a report to a processor (a service provider such as a cloud storage provider or a tool to manage the reports) may take place on the basis of the company's legitimate interest in efficiently processing these data with a view to the management of the reports, guaranteeing anonymity, access management etc.;

Your personal data will not be transferred to third countries that do not provide an adequate level of protection of your personal data.

You can always send an email to PZ@detraay.com if you have any further questions with respect to the guarantees as to the protection of your personal data and with respect to the processing of your personal data within the context of the whistleblowing policy, or if you want to exercise your right of access to, rectification, transferability or erasure of your personal data, provided that the exercise of these rights falls within the scope of the applicable legal provisions.

If, after having contacted the company, you still want to file a complaint relating to the processing of your personal data, you can address the competent supervisory authority, i.e. the Data Protection Authority.