Whistleblower policy

F.T.I vzw

Contents

Article 1. Why have a whistleblower policy?

The aim of this whistleblower policy is to make it possible for both internal employees and third parties (hereinafter: whistleblowers) who become aware in a work-related context of breaches of European Union law or breaches added by the Belgian legislators to the scope of the Belgian Law on whistleblowers (see the list under Article 3 below) committed by internal employees, external workers, customers or suppliers, to report such matters without fear of retaliation.

F.T.I vzw has set up an internal reporting channel for this purpose. Anyone wishing to make a report within the scope of the Law on whistleblowers will initially use the internal reporting channel.

Article 2. Definitions

In this policy the terms used are defined as follows:

Breaches: acts or omissions that:

- are unlawful and concern Union acts and policies falling within the substantive scope referred to in Article 3, or
- undermine the purpose or application of the rules in the Union act and policy areas falling within the substantive scope referred to in Article 3.

Information about breaches: information, including reasonable suspicions, about actual or possible breaches that have occurred or are very likely to occur within F.T.I vzw where the whistleblower works or has worked or with which the whistleblower has been in contact due to his/her work, as well as about attempts to conceal such breaches.

Reporting/report: the provision of information about breaches orally or in writing.

Internal reporting/report: the communication of information about breaches orally or in writing within F.T.I vzw.

External reporting/report: the communication of information about breaches orally or in writing to the competent authorities.

Disclosure: the public communication of information about breaches orally or in writing.

Whistleblower: a natural person who reports information (internally, externally or publicly) about breaches that he/she has obtained in the context of his/her work-related activities.

Person concerned: a natural or legal person named in the (internal, external or public) report or disclosure as a person to whom the breaches are attributed or with whom that person is associated.

Facilitator: a natural person who assists a whistleblower in the reporting process in a work-related context, and whose assistance should be confidential.

Retaliation: a direct or indirect act or omission that takes place in a work-related context following an internal or external report or disclosure, and that leads or could lead to an unjustified disadvantage for the whistleblower (or for the facilitators or third parties connected to the whistleblower).

Follow-up: any action taken by the recipient of a report or a competent authority to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported.

Feedback: the provision to the whistleblower of information on the action envisaged or taken as follow-up and on the grounds for such follow-up.

Competent authority: the Belgian authority designated to receive reports in accordance with Article 5 of this policy and to provide feedback to the whistleblowers and ensure follow-up.

Work-related context: current or past work activities in the private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information.

Federal coordinator: the authority responsible for coordinating external reports for the private sector in accordance with Section 4 Chapter 4 of the Law on whistleblowers.

Whistleblowing officer: the impartial person or service authorised to follow up on reports, maintain communication with the whistleblower, request additional information from him/her if necessary, provide him/her with feedback and receive reports if applicable.

Article 3. Reporting

The internal reporting channel is accessible 24/7 for:

- internal employees and external workers
- anyone who, in a work-related context, becomes aware of breaches of European Union law and/or breaches added by the Belgian legislators now or at some future time to the scope of the Belgian rules on whistleblowers.
- others: (e.g. customers, suppliers, etc.)

'Work-related context' means that in addition to current and former employees, interns, suppliers, self-employed persons, shareholders, job applicants, etc. who collaborate for a significant length of time with F.T.I vzw may also make a report.

In concrete terms, a whistleblower may report breaches or matters that he/she believes in good faith to constitute a breach in any of the following areas:

- government contracts;
- financial services, products and markets, prevention of money laundering and terrorist financing;
- product safety and product compliance;
- transport safety;
- protection of the environment;
- radiation protection and nuclear safety;
- food and animal feed security, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data, and the security of network and IT systems;
- breaches harmful to the financial interests of the European Union;
- breaches relating to the internal market (competition and state aid; corporate tax violations; schemes aimed at obtaining an unjustified tax advantage).
- combating tax fraud;
- combating social security fraud;
- application of the Good Governance Charter, internal company policies, employment regulations and delegation decisions.

Article 4. Internal reporting

4.1 Reporting channel and access

Any person who discovers a breach or has reasonable suspicions that a breach has occurred or will occur in one or more of the areas mentioned in Article 3, and in which F.T.I vzw is involved, may report this at any time through the most appropriate and accessible channel.

Within F.T.I vzw, a whistleblower has the following options for doing this:

- Making a telephone report to the HR employee(s) on telephone number 015/34 20 00
- Making a report by email to the HR employee(s) at personeelsdienst@technopolis.be
- Making a report via the website www.technopolis.be/en/legal/

Whistleblowers may also ask to report a breach at a physical meeting within a reasonable period of time. Such a physical report may also be made by appointment with the HR employees and may be requested by email or telephone.

4.2 Handling of internal reports

The internal reporting channels at F.T.I vzw are managed internally (and not externally).

The whistleblower will receive confirmation of receipt no later than seven days after receipt of the report.

An impartial person or department will be responsible for following up on the report and communicating with the whistleblower. The following persons or services within F.T.I vzw are eligible for this role:

All HR department employees (with the exception of the HR manager and/or HR director)

The risk of conflicts of interest in this context will be reduced to a strict minimum. If necessary, external investigative resources may be used.

4.3 Disclosure to government agencies

If a report contains information that must be passed on by law to a government agency responsible for monitoring crimes within the areas of Article 3 above, the person or service that follows up on the report within F.T.I vzw must forward the information to the government agency concerned.

4.4 Feedback

The whistleblower will receive feedback about the handling of the report. This means that he/she will receive information about what corrective measures, process improvements or changes and/or other further steps have been undertaken or not undertaken. This feedback will not contain details about specific individuals and may therefore be more general in nature.

If additional investigation is necessary or appropriate, the HR employee must ensure the confidentiality of the investigation and compliance with the rights of third parties.

Within a reasonable period, and no later than three months after confirmation of receipt has been sent, or, if no confirmation of receipt has been sent to the whistleblower, no later than three months after a period of seven days has elapsed since the report was made, the whistleblower will receive information about the measures planned or undertaken by way of follow-up and the reasons for that follow-up.

If it is not possible to provide the whistleblower with any feedback, the whistleblower will be notified of this, and of the reason why no information is yet available.

Article 5. External reporting

5.1 External reporting channels

A whistleblower who does not want to report internally may also use an external reporting channel. External reports are made to the federal coordinator of the competent authority (see Appendix 1 for the various contact details of the authorities). The whistleblower has the following options:

- Make a telephone report on a telephone number depending on the department – see Appendix 1
- Make a report by email depending on the department – see Appendix 1
- Make a report via the website of the competent authority depending on the department – see Appendix 1

  (e.g. integration of the tool on the competent authority's website)

The whistleblower may also ask to report a breach at a physical meeting within a reasonable period of time. Such a physical report may be made by appointment with the federal coordinator of the competent authority.

For more information: see Appendix 1.

5.2 Handling of external reports

The whistleblower will receive confirmation of receipt from the competent federal service no later than seven days after receipt of the report.

Within a reasonable period, and no later than three months after confirmation of receipt has been sent, or, if no confirmation of receipt has been sent to the whistleblower, no later than three months after a period of seven days has elapsed since the report was made, the whistleblower will receive information from the competent federal service about the measures planned or undertaken by way of follow-up and the reasons for that follow-up.

In exceptional, justified cases, this period may be six months.

The competent authorities and the federal coordinator will designate the personnel members responsible for handling reports, and in particular for:

- providing information about the reporting procedures to interested parties
- receiving and following up on reports
- maintaining contact with the whistleblower in order to provide feedback and request further information if necessary.

These personnel members are bound by a duty of confidentiality and will receive specific training in handling reports.

Article 6. Disclosure

Persons who make a disclosure are eligible for protection under the Law on whistleblowers if the following conditions are met:

1. in the case of indirect disclosure: if the person has first made an internal and/or external report, but no appropriate measures have been taken as a result of that report within the set period; or
2. in the case of direct disclosure: the person has reasonable grounds to believe that:
   - the breach may constitute an imminent or manifest danger to the public interest; or
   - there is a risk of retaliation if an external report is made, or the breach is unlikely to be effectively remedied due to the particular circumstances of the case, for example because evidence may be withheld or destroyed, or an authority may collude with the perpetrator of the breach or is involved in the breach.

This does not apply to cases where a person provides information directly to the press under specific provisions establishing a system for the protection of freedom of expression and information.

Article 7. Confidentiality and secrecy

F.T.I vzw will ensure that any information about the report is stored in such a way that it is physically and digitally accessible only to those

designated by F.T.I vzw as authorised persons. All reports and subsequent investigation and/or assessment reports, decisions, etc. must be treated with the utmost confidentiality.

F.T.I vzw applies a strict ‘need to know’ basis for disclosing relevant information to employees or third parties. All employees involved in the receipt of or follow-up on reports will maintain strict confidentiality regarding the content of whistleblowers’ reports, investigation and/or assessment reports, decisions, etc. to the extent permitted by applicable law.

Article 8. Protection

8.1 Protection against retaliation

F.T.I vzw will ensure that all whistleblowers are protected against retaliation, including threats and attempted retaliations (see below), if the whistleblower acts in good faith and follows the correct procedure when making a report. The 'correct procedure' means that where possible the whistleblower initially uses the internal reporting channels that have been provided. Only if there is no internal channel, or if there is no follow-up on an external report, may a report be made publicly.

By 'retaliation' we mean, among other things:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or employment reference;
- the imposing or applying of a disciplinary measure, reprimand
- or other sanction, such as a financial sanction;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial
- loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

In addition to the whistleblower him-/herself, the facilitators and third parties associated with the whistleblower who may also be victims of retaliations in a work-related context, and any accused individuals, are also protected. F.T.I vzw will safeguard their right to due process and the presumption of innocence. Their identity will be kept strictly confidential while investigations into the report are ongoing.

8.2 Complaints procedure

Any whistleblower who believes he or she is a victim of retaliations or is being threatened with retaliations may submit a substantiated complaint to the federal coordinator of the competent authority, who will initiate an extrajudicial protection procedure.

The federal coordinator of the competent authority will verify the existence of reasonable suspicion of retaliations.

The burden of proof regarding the absence of retaliations falls on F.T.I vzw.

If F.T.I vzw takes a measure against a whistleblower that falls within the legal framework, and F.T.I vzw can demonstrate that the reasons for that measure have nothing to do with the report, then that measure does not constitute a retaliation.

Article 9. Abuse of reporting channels / breaches of this policy

F.T.I vzw will only handle reports that have been made in good faith and that fall within the scope of the Law on whistleblowers. Employees who make a report in bad faith, with the intention of causing harm, are not protected.

If an employee makes a report in bad faith, that employee is in particular liable to incur the sanctions set out in the employment regulations, including the ultimate measure of dismissal.

Article 10. Retention of documents / register of whistleblowers' reports

F.T.I vzw keeps a register of all whistleblowers' reports, in which an up-to-date record is kept of the receipt of the report, the investigation and its resolution. The reports are kept in this register for the duration of the contractual relationship between the whistleblower and the employer.

Investigation reports and supporting information will be kept for at least five years after the end of the investigation.

Article 11. Processing of personal data

The data controller is F.T.I vzw, with registered office at Technologielaan 1 - 2800 Mechelen, company number 0434 183 579.

All personal data will be processed in accordance with applicable data protection laws, including the General Data Protection Regulation ('GDPR').

Personal data will be processed exclusively for the purpose of carrying out the required investigations on the basis of a legal obligation, and only strictly necessary data will be processed. The data may be shared with government agencies if the report contains information that is legally required to be passed on, or with other external parties involved in an investigation.

F.T.I vzw will store all personal data at least for as long as the contractual relationship between the whistleblower and the employer exists, and at most for the limitation period that is relevant for any legal claims.

All data subjects have the right to make a request for access, rectification or erasure of their personal data and to object to the processing of such data. Such requests may be addressed to the HR employee(s).

All data subjects have the right to submit a complaint to the Data Protection Authority.

The data protection officer at F.T.I vzw can be reached at **info@technopolis.be.**

Article 12. Support measures

The Federal Institute for the Protection and Promotion of Human Rights is responsible for applying or overseeing the support measures, in the case of internal reports, external reports and disclosures.

The whistleblower has access to the following support measures, as appropriate:

- complete and independent information and advice, easily accessible and free of charge, on the remedies and procedures available to protect against retaliations, as well as on the rights of the person concerned, including his/her rights to the protection of personal data; the whistleblower must also be informed that he/she is eligible for the protection measures provided for by this law;
- technical advice from any authority involved in the protection of the whistleblower;
- legal aid in cross-border criminal and civil proceedings in accordance with Directive (EU) 2016/1919 and Directive 2008/52/EC of the European Parliament and of the Council and legal aid in other proceedings as well as legal advice or other legal assistance, in accordance with the provisions on second-line legal assistance and legal aid;
- support measures, including technical, psychological, media-related and social support, for the whistleblower;
- financial assistance to the whistleblower in connection with legal proceedings.

Appendix I: List of federal authorities

1 Government contracts: the Public Procurement Service of the FPS Chancellery of the Prime Minister;

2 Financial services, products and markets, prevention of money laundering and terrorist financing: the FSMA for the rules referred to in Article 45 of the Law of 2 August 2002, the NBB for the rules referred to in Articles 12bis and 36/2 of the Law of 22 February 1998, the Belgian Audit Oversight Board for the rules referred to in Article 32 of the Law of 7 December 2016;

3 Product safety and product compliance: FPS Economy, FPS Public Health, the FAMHP, the BIPT, FPS Mobility;

4 Transport safety: FPS Mobility, National Authority for Maritime Security;

5 Protection of the environment: FPS Public Health, Food Chain Safety and Environment, Brussels Environment, CREG, the Directorate-General Energy, ACER;

6 Radiation protection and nuclear safety: Federal Agency for Nuclear Control;

7 Food and animal feed security, animal health and welfare: the FASFC, FPS Public Health, Food Chain Safety and Environment;

8 Public health: Sciensano, FPS Public Health, Food Chain Safety and Environment, the FAMHP, Federal Commission for Patients' Rights;

9 Consumer protection: FPS Economy;

10 Protection of privacy and personal data, and the security of network and IT systems: the Data Protection Authority, the CCB, the EDPS.