WHISTLEBLOWING POLICY

Date of issuance : 1 January 2024
Lastly updated :

Table of contents

1 Introduction

The Belgian law of 28 November 2022 on the protection of persons who report breaches of Union or national law within a legal entity in the private sector (the "**Whistleblowing Law**") requires the establishment of an internal reporting channel for the purpose of whistleblowing.

The objective of this policy (the "Whistleblowing Policy") is to:

(i) ensure the establishment of an internal whistleblowing channel in accordance with the applicable legal requirements;

(ii) facilitate and encourage the reporting of abuse and misconduct, such as irresponsible behaviour, corruption, fraud, money laundering, market abuse, *etc*;

(iii) ensure that persons reporting such abuse or misconduct and their associates are protected against possible negative consequences or disciplinary action that may result from the reporting.

2 Scope of application of this policy

2.1 Legal entities under scope

The Whistleblowing Policy applicable to the following legal entities :

(i) TDP NV

(ii) TINC Manager NV

(iii) Any legal entity in which the entities under (i) and/or (ii) have a mandate as statutory director

(each of those legal entities "**a Company**")

2.2 Persons who can report a breach

Any person who works for or with the Company in a work-related context can report a breach. That includes the following persons:

- prospective employees, current employees (whether on a temporary or permanent contract, and whether working on site or from home), or former employees of the Company;
- current or former self-employed individuals, persons working under the supervision and direction of contractors, sub-contractors and suppliers, who have worked full-time or part-time with or for the Company;
- current and former shareholders and individuals belonging to the administrative, management, or supervisory body of the Company, including non-executive members;
- current and former applicants, volunteers, trainees and interns of the Company (whether paid or unpaid).

By exception, any person – irrespective of whether they find themselves in a work-related context – can report a breach regarding rules in the areas financial services, products, and markets (including the Market Abuse Regulation), or related to the prevention of money laundering and terrorist financing.

The persons referred to above will hereinafter be referred to as the "**whistleblower**".

At the time of reporting, the whistleblower must have reasonable grounds to believe that the information on which they base the report is true, and that is falls within the scope of the breaches that can be reported under this policy.

2.3 Breaches that can be reported

Any whistleblower is entitled to report breaches of laws or regulations by the Company. There are different types of breaches that can be reported, namely:

(i) breaches of financial markets regulations that specifically apply to the Company as a listed company (see 2.3.1 below);

(ii) breaches of other laws and regulations that can be reported under the Whistleblowing Law (see 2.3.2 below); and

(iii) breaches falling out of the scope of those areas (see 2.3.3 below).

Regarding all of those areas, breaches that can be reported are not limited to active or past violations or infringements, but also include omissions, breaches for which a person has specific reasons to suspect that they will take place and attempts to commit or conceal breaches.

2.3.1 *Breaches of financial market regulations*

As an issuer of financial instruments, the Company is subject to disclosure requirements set in the Market Abuse Regulation. In particular, the Company must:

- publicly disclose inside information;
- draw up a list of persons having access to inside information ("**insider list**");
- report on transactions carried out by its managers.

2.3.2 *Breaches that can be reported under the Whistleblowing Law*

The law provides for the protection of whistleblowers reporting breaches of laws and regulations related to or affecting:

- financial services and products;
- the prevention of money laundering and terrorist financing;
- public procurement and the award of concessions and contracts;
- product safety and compliance;
- transport safety;
- the protection of the environment;

- nuclear safety or protection against harmful radiation;
- food and feed safety, and animal health and welfare;
- public health;
- consumer protection;
- the protection of privacy and personal data, and security of network and information systems;
- the financial interests of the Union;
- the internal market, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of applicable corporate tax law;
- the fight against tax fraud and social security fraud.

2.3.3 *Other breaches*

Breaches falling out of the scope of the areas set out above can still be reported and will be treated on a strictly confidential basis by the Company in accordance with the arrangements set out in this policy. That includes e.g. breaches related to immoral and/or unethical behaviour, including transgressive behaviour, infringement of ethical policies.

-

3 How to report

Whistleblowers are entitled to use any of the reporting channels defined below and are free to choose the reporting channel they consider the most appropriate.

3.1 Internal reporting

Reporting can be carried out internally by sending an email to Compliance@tdpartners.com. Whistleblowers shall not be required to share their identity details and are entitled to use an anonymised email addresses for the purpose of reporting internally.

Regarding the Company email account for whistleblowing, the Company shall ensure that:

- the person who receives the internal report via email shall be independent and free from conflicts of interest;
- the account shall be operated in a secure manner, ensuring that the confidentiality of the identity of the whistleblower and any third party mentioned in the report is protected;
- the account cannot be accessed by any other, non-authorised staff members.

The recipient of the report shall:

- acknowledge receipt of the report to the whistleblower within seven days of receipt, via the email address used by the whistleblower to submit the report;

- be responsible for diligently following up on the report and maintain communication with the whistleblower and, where necessary, ask for further information from the whistleblower;
- provide feedback to the whistleblower within a reasonable timeframe, not exceeding three months from the day the report was made;
- provide clear and easily accessible information regarding the procedures for reporting externally to competent authorities;
- not disclose the identity of the whistleblower – or any other information from which the identity of the whistleblower may deduced directly or indirectly – to anyone else without the explicit consent of the whistleblower, unless such disclosure would be required in the context of investigations by national authorities or judicial proceedings;
- keep an internal, confidential record of every report received, which shall only be accessible by the recipient of the report, and which shall be protected against unauthorised access by any other person.

The Company shall be the controller of the personal data processed for the purposes of internal reporting and must ensure compliance with all relevant data protection laws and regulations (in particular, the GDPR). the Company shall not collect personal data which are manifestly not relevant for the handling of a specific report or, if accidentally collected, it shall delete such data immediately.

3.2 External reporting

Whistleblowers have the right to report directly – that is, without first reporting internally – to an external reporting channel. They also preserve the right to report externally where an internal report has already been made.

Annex 1 to this policy sets out a list of competent authorities to which an external report can be made, depending on the area of the breach concerned. The FSMA is competent to receive external reports on breaches of the Market Abuse Regulation. The applicable rules and procedures for making an external report to the FSMA can be found on its whistleblowing webpage.

3.3 Public disclosure

Whistleblowers may decide to make a public disclosure of information related to a breach by the Company. In that case, whistleblowers only benefit from legal protection if:

(i) they first reported internally and externally, or directly externally, but reports were not dealt with, or no appropriate action was taken, within three months from the receipt of the report; or

(ii) they have reasonable grounds to believe that:

- the breach may constitute an imminent or manifest danger to the public interest (*e.g.*, an emergency situation or a risk of irreversible damage); or
- in the case of external reporting, there is a risk of retaliation or there is a low

prospect of the breach being effectively addressed due to particular circumstances (*e.g.*, circumstances where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator or involved in the breach).

4 Protection of whistleblowers

The Company shall in all circumstances refrain from taking any form of retaliation against whistleblowers, including threats of retaliation and attempts of retaliation including in particular in the form of:

(a) suspension, lay-off, dismissal or equivalent measures;

(b) demotion or withholding of promotion;

(c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

(d) withholding of training;

(e) a negative performance assessment or employment reference;

(f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

(g) coercion, intimidation, harassment or ostracism;

(h) discrimination, disadvantageous or unfair treatment;

(i) 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;

(j) failure to renew, or early termination of, a temporary employment contract;

(k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;

(l) 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;

(m) early termination or cancellation of a contract for goods or services;

(n) cancellation of a licence or permit;

(o) psychiatric or medical referrals.

Whistleblowers who feel the victim of such retaliation, including threats or attempts of retaliation, have the right to file a complaint with the Federal Ombudsman.

The protection measures set out herein apply not only to the whistleblower, but also to:

- facilitators (that is, any natural person who assists a whistleblower in the reporting process, and whose assistance should be confidential);

- third persons who are connected with the whistleblower and who could suffer retaliation, such as colleagues or relatives of the whistleblower; and
- legal entities that the whistleblower owns, works for or is otherwise connected with in a work-related context.

5 Policy updates

This policy shall be updated regularly and at least on an annual basis.

Annex 1 – List of competent authorities for external reporting

The authorities that are competent to receive internal reports are:

1° de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;

2° de Federale Overheidsdienst Financiën;

3° de Federale Overheidsdienst Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu;

4° de Federale Overheidsdienst Mobiliteit en Vervoer;

5° de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;

6° de Programmatie Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid

7° het Federaal Agentschap voor Nucleaire Controle;

8° het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;

9° het Federaal Agentschap voor de veiligheid van de voedselketen;

10° de Belgische Mededingingsautoriteit;

11° de Gegevensbeschermingsautoriteit;

12° de Autoriteit voor Financiële diensten en Markten;

13° de Nationale Bank van België;

14° het College van toezicht op de bedrijfsrevisoren;

15° de autoriteiten gemeld in artikel 85 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

16° het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater;

17° het Belgisch Instituut voor postdiensten en telecommunicatie;

18° het Rijksinstituut voor ziekte- en invaliditeitsverzekering;

19° het Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen;

20° de Rijksdienst voor Arbeidsvoorziening;

21° de Rijksdienst voor Sociale Zekerheid;

22° de Sociale Inlichtingen en Opsporingsdienst;

23° de Autonome dienst Coördinatie Anti-Fraude (CAF);

24° de Scheepvaartcontrole.