1 INTRODUCTION

A whistleblower policy is a policy set up by a private or public organization with the aim of providing both employees and third parties with the opportunity to report certain facts that they believe violate applicable laws or regulations without fear of retaliation.
Contec BV is setting up an internal reporting channel for this purpose.

The whistleblower policy applies to legal entities with at least 50 employees and is therefore only mandatory for Contec BV.

2 NOTIFICATIONS

Anyone who becomes aware of breaches of European Union law and/or breaches that the Belgian legislator has added or will add to the Belgian whistleblower scheme in a work-related context has various channels available to report a breach:

- internal reporting channel
- external reporting channel
- publication

'Work-related context' means that in addition to (former) employees, trainees, self-employed persons, partners, applicants, suppliers, etc. who work together with Contec BV in a sustainable way.

Specifically, a reporting person can report breaches or matters that he believes in good faith to constitute a breach in one of the following areas:

- public procurement;
- 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 feed safety, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data, and security of network and information systems;
- infringements relating to the internal market of the European Union such as infringements of state aid and competition rules: anti-competitive practices and agreements, abuse of pricing, abuse of dominant position, etc.;
- tax evasion;
- combating social fraud;
- affecting the financial interests of the Union.

2.1 Internal notification

2.1.1 Internal reporting channel

A person who notices a breach can report this in writing via the internal reporting channel of Contec BV. The reporting form can be found on the homepage of intranet.

A report must contain at least the following information:

- name, address, position and contact details of the reporting person;
- date of the report;
- a detailed description of the (alleged) infringement, such as:
    - a description of the (alleged) infringement;
    - possibly with annexes (documentation or supporting documents);
    - the identification of the possible data subject(s) or departments of the company;
    - where the infringement occurred;
    - when the infringement took place;
    - how and when the reporting person noticed or was notified of the breach;
    - the relationship with the company (employee, freelancer, supplier, shareholder, etc.);
    - the impact of the incident (for the company, for the public interest, etc.);
    - any other relevant information regarding the (alleged) infringement.

Reporters can also request to report a breach to the reporting responsible of Contec BV within a reasonable period of time via a physical meeting. Such a physical meeting always takes place by appointment.

2.1.2 Handling of internal reports

The internal reporting channel at Contec BV is managed internally.

The reporter will receive a confirmation of receipt no later than 7 days after receipt of the report.

Within Contec BV, Kathleen Van Mol and Anneli Van den Bergh will be responsible for the investigation and follow-up of the report as well as for the communication with the reporter as impartial reporting managers. The investigation is carried out within a reasonable time. As a general rule, a period of no more than 3 months after the acknowledgement of receipt applies.

2.1.3 Feedback

During the investigation and after the period of 3 months after the acknowledgement of receipt, the reporter receives general information about the progress and outcome of the investigation.

2.2 External notifications

2.2.1 External reporting channel

If no appropriate measures have been taken through the internal procedure, the reporter can report a breach via an external reporting channel of the government. The reporter can also immediately make a report via the government's external reporting channel.

The external reporting channel offers the possibility to make written and oral reports to the Federal Ombudsman. A verbal report is possible by telephone or via other voice messaging systems and, at the request of the reporting person, by means of a physical meeting within a reasonable time. The following webpage of the Federal Ombudsman contains more information about the reports to this external reporting channel: https://www.federaalombudsman.be/nl/centrum-integriteit/welke-meldingen.
The government's external reporting channel can be reached via the Federal Ombudsman at:

- e-mail (also to make an appointment) : integriteit@federaalombudsman.be
- telephone (also to make an appointment) : 02/289.27.04
- online report form : https://www.federaalombudsman.be/nl/meldingsformulier

2.2.2 Feedback

The independent external reporting channel of the Federal Ombudsman will send an acknowledgement of receipt within 7 days.
The external reporting channel will provide feedback to the reporting person within three months or, in special cases, six months, on the planned follow-up or measures taken and on the reasons for that follow-up, unless a legal provision prevents this. The external reporting channel will inform the reporter of the final outcome of the investigations.

2.3 Publication

A reporting person who makes a breach public by making information about breaches publicly available (e.g. via the media) is eligible for protection if the following conditions are met:

1. The reporting person has first made an internal or external report as prescribed under sections 2.1 or 2.2, but no appropriate measures have been taken;
2. The reporter has good reason to believe that:
   - the infringement may constitute an imminent or real danger to the public interest;
   - in the case of external reporting, there is a risk of retaliation, or the infringement 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 infringement or is involved in the infringement.

3 CONFIDENTIALITY AND SECRECY

Contec BV ensures that the information about the report is stored in such a way that it is physically and digitally only accessible to those who have been designated as authorized persons. All reports and subsequent investigation reports and/or determination reports, decisions, ... shall be treated with the utmost confidentiality. Contec BV has a strict 'need to know' basis for disclosing relevant information to employees or third parties. All employees involved in the acknowledgement of receipt, or follow-up of reports, will maintain strict confidentiality about the content of reports, reports, decisions, etc. to the extent permitted by applicable law.

4 PROTECTION AGAINST RETALIATION

Contec BV guarantees that the reporter is protected against retaliation, including threats and attempts at retaliation (see below), if the reporter acts in good faith and follows the correct path when making a report.

The "right way" means that the reporter initially makes use of the provided internal reporting channels as much as possible. Only if there is no internal channel, or if an external report remains without effect, can a report be made public.

By "retaliation" we mean, among other things:

- suspension, temporary dismissal, dismissal or similar measures;
- demotion, or refusal of promotion;
- transfer of tasks, change of location of the workplace, reduction of wages, change of working hours;
- withholding education;
- a negative performance assessment or employment reference

- imposing or applying a disciplinary measure, reprimand or other sanction, such as a financial penalty;
- coercion, intimidation, harassment or exclusion;
- discrimination, disadvantage or unequal treatment;
- failure to convert a temporary employment contract into an employment contract of indefinite duration, in the event that the employee had a legitimate expectation that he would be offered employment for an indefinite period;
- non-renewal or early termination of a temporary employment contract; damage, including reputational damage, in particular on social media, or financial loss, including loss of turnover and revenue;
- blacklisting on the basis of an informal or formal agreement covering an entire sector or industry, preventing the reporting person from finding a job in the sector or industry;
- early termination or termination of a contract for the supply of goods or services;
- revocation of a license or permit;
- psychiatric or medical referrals.

In addition to the reporting person himself, the facilitators and third parties associated with the reporting person who may also be victims of retaliation in a work-related context, as well as any accused individuals, are also protected. Contec BV guarantees them the right to a fair trial and the presumption of innocence. Their identity will be kept strictly secret as long as the investigations following the report are ongoing.

Any reporting person who considers that he or she has been the victim of or threatened retaliation may submit a reasoned complaint to the federal coordinator of the competent authority, who will initiate an extrajudicial protection procedure. The federal coordinator of the competent authority verifies the existence of a reasonable suspicion of retaliation.
The burden of proof that it is not a retaliation is borne by Contec BV. If Contec BV takes a measure against a reporter who falls within the legal framework, and Contec BV can demonstrate that the reasons for that measure are unrelated to the report, then that measure is not a retaliation.

5 ABUSE OF THE REPORTING CHANNELS

Contec BV will only handle those reports that were made in good faith and that fall within the scope of the whistleblower policy. Employees who report in bad faith, with the intention of harming, are not protected. In the event of a report made in bad faith, the worker concerned is particularly exposed to the sanctions contained in the work regulations, including the ultimate measure of dismissal.

6 PROCESSING OF PERSONAL DATA

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

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

All data subjects have the right to request access, rectification, erasure of, and objection to the processing of their personal data. These requests can be addressed to info@contec-ias.com. All data subjects have the right to lodge a complaint with the Data Protection Authority.

7 RETENTION PERIOD

The personal data processed in the context of the reporting procedure will not be kept longer than necessary for the internal and/or external (police/judicial/administrative) investigation. In the event of police, administrative, judicial or disciplinary proceedings, the data will be archived after the expiry of the applicable limitation period or appeal period or stored for a maximum of two months thereafter.

8 COOPERATION MANAGEMENT

In order to ensure that this notification scheme is properly embedded, management will develop the following activities:

- ensure that this scheme is available and known to all employees;
- take all matters concerning reports of integrity violations very seriously, take timely action and guarantee confidentiality and care.