Policy
Whistleblowing at Berco

v. 1 14 July 2023

Summary.

Introduction.

At thyssenkrupp integrity, compliance with the law and internal regulations are of highest priority. To ensure that these values are upheld and potential risks arising from violations are avoided or minimized, it is crucial that misconduct is identified, clarified, and remedied at an early stage. Every indication of a potential misconduct will be treated seriously and will lead to an investigation following an objective and transparent process without any bias.

Violations of laws and internal regulations bear the risk of considerable damage to the tk Group, the Executive Board, every responsible executive at all levels within the Group as well as any involved employee. Besides large fines, which may even affect thyssenkrupp as a Group, acting individuals are threatened by external personal consequences, which may include fines or depending on the case even imprisonment, as well as internal personal consequences. Beyond that, compliance cases may lead to reputational and economic damage (e.g. negative media coverage, loss of turnover), damage claims (e.g. by customers) and exclusion from public tenders (“blacklisting“).

The Executive Boards of the group are legally obliged to investigate at their own initiative every suspicion of illegal or improper actions of which they are informed. Compliance violations and infringements of laws identified in this course have to be ceased immediately and sanctions have to be considered. Furthermore, the Executive Boards of the groups are obliged to verify if civil claims for damages can be made against the offender.

To comply with their legal obligations the Executive Boards of thyssenkrupp mandated Legal & Compliance Investigations (Compliance Investigations) to investigate all indications and allegations of possible compliance related misconduct. Besides that, information on violations outside the core compliance topics (corruption, antitrust law, data protection, money laundering, trade compliance) can be forwarded to the relevant departments or dealt with in cooperation with them. Information on violations of the International Framework Agreement (violations of global minimum labor standards at thyssenkrupp) is brought to the attention of the representatives on the International Committee and the Labor Relations department at thyssenkrupp AG and processed in consultation with them.

The presentation and explanation of the whistleblowing management system at thyssenkrupp is outlined in the policy **whistleblowing at thyssenkrupp** and takes into consideration the various legal requirements related to whistleblowing systems and whistleblower protection, such as the EU Directive 2019/1937 on whistleblowers, respective implementing laws, the Law on Corporate Diligence Obligations in Supply Chains (LkSG), etc.

Legislative Decree No. 24 of March 10, 2023, on the "Implementation of Directive (EU) 2019/1937 (hereinafter the "Decree"), implemented the EU Directive by significantly extending the scope of application of the reporting regulations, which were previously limited, for the private sector, only to entities with an Organization, Management and Control Model pursuant to Legislative Decree 231/2001.

Specifically, the Decree identifies and regulates the Whistleblowers, the subject matter of violation reports, the channels to be established and provided for, and the obligations and safeguards that companies are required to implement and guarantee, and also defines the criteria and timelines for compliance.

Berco SpA, in fulfillment of its obligations under the Decree, has adopted a whistleblowing platform dedicated to its own reality, alongside the group platform, the management of which is entrusted to the Supervisory Board of Berco SpA, established pursuant to Legislative Decree 231/01 and subsequent

amendments (SB). This document Whistleblowing in Berco is intended to illustrate and define the methods and conditions of use of Berco's whistleblowing platform and other internal reporting channels.

Berco and the group coordinate their actions to ensure that reports, regardless of the channel used by the person wishing to report wrongdoing, are handled by the most appropriate channel and body or function for the best handling of the report.

Whistleblower information helps thyssenkrupp to counteract violations at an early stage, and to reduce the damage caused to our company, our employees, and our business partners.

Definitions

Work context	Present or past employment or professional activities through which, regardless of the nature of such activities, a person acquires information on Violations and in the context of which he/she could risk retaliation in the event of a Report or public disclosure or a complaint to the judicial or accounting authorities
Facilitator	The person assisting a Whistleblower in the reporting process, whose identity is protected in the same way as that of the Whistleblower himself
Reporting Manager	The person or team of persons, internal or external to Berco, identified for the management of Reports
Information on violations	Information or well-founded suspicions of violations that have been committed or may be committed in our organisation
Person Involved/Signalled Person	The person named in the Report, or in the public disclosure, as the person to whom the breach is attributed, or the person otherwise implicated in the reported or publicly disclosed breach
Feedback	Communication to the reporter on how the report has been or will be handled
Retaliation	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the report, the complaint to the judicial or accounting authorities, or the public disclosure, which causes or may cause the Whistleblower, directly or indirectly, unfair harm
Company	Berco SpA with registered office in Copparo (FE), via I Maggio 237
Reporting person(s) / Whistleblower	The person making the Report or public disclosure of information on violations acquired within his or her work context
Report(s)	The written or oral communication of information on Violations
Private sector actors	Subjects, other than those falling within the definition of public sector subjects, which: (i) have employed, in the last year, an average of at least 50 (fifty) subordinate workers with fixed-term or open-ended employment contracts; (ii) fall within the scope of application of European Union acts, even if in the last year they did not reach the average of 50 (fifty) subordinate workers; (iii) adopt Organisation, Management and Control Models provided for by Legislative Decree 231/2001
Public sector actors	The public administrations referred to in Article 1(2) of Legislative Decree 165/2001, the independent administrative authorities responsible for guaranteeing, supervising or regulating, public economic bodies, bodies governed by public law, public service concessionaires, publicly controlled companies and *in-house* companies
Violations	Actions or behaviour contrary to our internal policies and the law, as further identified under 4 below
Whistleblowing	The process of reporting offences involving violations pursuant to Legislative Decree 24/2023

01. Scope.

Who can inform about a violation?

The Whistleblower is the natural person who makes the Report or public disclosure of information on Violations acquired in the context of his or her work.
Reporting can be done in Berco's reporting channel by all of the following:

- staff with an employment relationship
- self-employed workers
- freelancers and consultants, suppliers
- volunteers and trainees
- shareholders or owners of company shares
- persons with administrative, management, supervisory or representative functions.

What can be reported?

Violations are defined as all actual or potential conduct, acts or omissions that damage the public interest or the integrity of the Company, and consist of:

(i) unlawful conduct relevant under Legislative Decree 231/2001 and violations of Model 231;
(ii) offences falling within the scope of the European or national legislation set out in the Annex to the Decree or the domestic legislation implementing the European Union acts set out in the Annex to Directive (EU) 2019/1937 (albeit not included in the Annex to the Decree), relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;
(iii) acts or omissions detrimental to the financial interests of the European Union (e.g. fraud, corruption and any other illegal activity related to European Union expenditure);
(iv) acts or omissions concerning the internal market (e.g. competition and state aid violations);
(v) acts or conduct that frustrate the object or purpose of the provisions of the acts of the European Union.
(vi) acts or omissions affecting the financial interests of the European Union;
(vii) acts or omissions affecting the internal market, including violations of EU competition and state aid rules.

They may not be reported, publicly disclosed or denounced:

- disputes, claims or demands linked to a personal interest of the Whistleblower that relate exclusively to his/her individual employment relationships, or inherent to his/her employment relationships with hierarchically superior figures;
- national defence and security alerts;
- reports on violations already regulated in some special sectors (financial services; prevention; money laundering; terrorism; transport safety; environmental protection).

The Report must not take an insulting tone or contain personal offence. The use of such expressions may be submitted by the Reporting Manager to the competent corporate functions for appropriate assessments, including disciplinary ones.

Who is responsible for the whistleblower system?

The responsible for receiving reports through Berco's reporting channel is the Organismo di Vigilanza (Supervisory Body) established pursuant to Legislative Decree 231/01 and subsequent amendments (hereinafter the Reporting Manager). The Supervisory Board has the requirements of independence, professionalism, honourableness and continuity of action such as to ensure that the processing of the report is carried out in accordance with the criteria of impartiality, independence and confidentiality.

The Supervisory Board may make use of external consultants and liaise with the Compliance Investigation function. In particular, it will follow up directly those cases falling within the perimeter of Legislative Decree 231/01, while it will entrust Compliance Investigation with those cases of violations of national and European regulations that fall outside the 231 perimeter.

Information on violations outside the core topics of compliance and Legislative Decree 231/01 will be forwarded by the Supervisory Board to the relevant departments or processed in cooperation with them, depending on the individual case.

Anonymity and Confidentiality.

Whistleblower anonymity in reporting is permitted, provided they contain the essential elements set out in Chapter 3.

Protection of the Whistleblower (Non-Retaliation).

Berco strictly prohibits and does not tolerate any kind of retaliation for reporting a violation in good faith or for otherwise cooperating in an investigation of a violation. See paragraph 5 below for more details.
Any violations should be reported using one of the reporting channels outlined in this Policy.
Reporting knowingly false information ('malicious reporting') is a violation Itself and measures taken as a consequence of such malicious reporting are not acts of retaliation.

Others persons concerned.

During its investigations, Berco strives to protect the legitimate interests of other persons affected by a disclosure (including those of accused persons). Casting suspicion on another person can have serious consequences. thyssenkrupp strictly follows “presumption of innocence” and “need to know” principles during investigations. It is essential that the Whistleblowing System is used responsibly. Berco will not support actions based on which employees may fall victim to groundless, or false allegation

02. Internal reporting channels.

Berco makes a number of whistleblowing channels available which are set out below:

1. Reporting in writing via the whistleblowing platform

The Company has adopted a platform for whistleblowing reports (hereinafter also referred to as the 'WB Platform'), provided by a specialised service provider.

The WB Platform is structured to ensure that:

- during the reporting process, the information acquired respects the principles of personal data protection and maximum confidentiality. This is achieved through the adoption of encryption techniques and the implementation of technical-organisational security measures defined, assessed and implemented also in the light of an impact assessment pursuant to Article 35 of the GDPR;
- Relevant information is accessible only to the Reporting Manager, and within which only to persons who have received specific authorisation;
- is continuously available 24 hours a day, 7 days a week.

When submitting a report, the WB Platform provides a token (Report ID) that allows you to check the status of the report, obtain information on the outcome and, if desired, communicate anonymously with the Report Manager.

The WB Platform allows internal functions involved in reporting to be excluded from the management of activities.

Only the Reporting Manager is allowed access to the Reports, to the relevant information and to the documents contained in the Platform. However, depending on the content of the Report, the Manager may deem it necessary to involve the other actors of the Company's internal control system, who, consequently, may be involved in the investigation, while fully respecting the confidentiality of the identity of the Reporting Party, of the person possibly involved and of the reported person, as well as of the content of the Report and of the relevant documentation.

As mentioned above, if the reporter has accessed the Platform anonymously, he/she must remember the unique key in order to be able to continue interacting on the same file through the Platform.

Otherwise, he will be able to access and interact on the same file using the username and password that he may have generated at the time of access.

The process of the file, with its attached information and documents, is tracked on the platform.

2. Written notification by paper mail

The Report may be made in writing by means of correspondence addressed to the Reporting Manager to be sent to the Berco S.p.A. offices by ordinary mail addressed to: Organismo di Vigilanza BERCO S.p.A. c/o BERCO SPA via I° Maggio 237 44034 Copparo (FE). with the wording "confidential".

3. Oral reporting via the Voice Messaging System

Reporting can be done via the WB Platform by leaving a voice message.

The Report is documented by the Reporting Manager in writing by means of a detailed transcript of the conversation. The Reporting Party may verify, rectify and confirm the content of the transcript by signing it.

4. Reporting by request for a face-to-face meeting

A Report may be made by requesting the setting up of a direct meeting with the Reporting Manager, conveyed through one of the established Internal Channels. This meeting should be organised within a reasonable time.

In such a case, with the consent of the reporting person, the Report is documented by the Reporting Manager, either by means of a recording on a device suitable for storage and listening, or by means of minutes. In the case of minutes, the reporting person may verify, rectify and confirm the minutes of the meeting by signing them.

03. The Report.

1. The elements of the Internal Reporting Channel.

You must provide all the elements that are useful and necessary to enable the Reporting Manager receiving the Report to conduct an investigation, to carry out the appropriate checks and investigations, and to assess the admissibility and merits of the Report.
In order to provide the Report, you do not need to have proof of the breach; however, you do need to have sufficiently circumstantial information to make it reasonable to submit it.
The Report must contain the following elements:

- your personal details, including your job title and/or function/activity within the Company (these details will be kept confidential). You may also choose to disclose your identity at a later stage, although it may be easier to handle the Report with your immediate identification. You may also report anonymously;
- a clear and complete description of the facts, as precise and concordant as possible, which are the subject of the Report and which constitute or may constitute a relevant Breach
- if known, the circumstances of time and place in which the facts that are the subject of the Report were committed;
- if known, the personal details or other elements enabling identification of the person and/or persons who have carried out the reported facts (e.g. position held and area of activity)
- an indication of any other persons who may report on the facts that are the subject of the Report
- an indication of any documents that may confirm the facts that are the subject of the Report
- any other information that may provide useful feedback as to the existence of the facts that are the subject of the Report and in general any other information or document that may be useful to understand the facts reported.

2. Types of Reporting.

Incomplete reports

If the Report is unsubstantiated, and does not allow sufficient elements to be identified to start an investigation (e.g. lack of the offence committed, reference period, causes and purposes of the offence, persons/functions involved, etc.), the Reporting Manager in charge of receiving the Report will ask you for additional information, in order to follow up the Report.

Not relevant

Reporting is not relevant to the scope of this Policy, because it relates to external parties or to facts, actions or conduct that are not subject to reporting under applicable law.
If the Reporting Manager considers that the Report is well-founded and circumstantiated, even if not relevant for his purposes, he may proceed to bring the Report to the attention of the competent internal function, always taking care to maintain the confidentiality of the identity of the reporter.
If your protection cannot be guaranteed, the Report will only be forwarded with your express consent.

Relevant report but not negotiable

The Report is relevant to the scope of this Policy, but at the end of the preliminary examination phase and the possible request for further information, it was not possible to gather sufficient information and elements about the Report to be able to proceed with further investigation.

Relevant and treatable report

The Report is relevant to the scope of this Policy, and sufficient information and evidence can be gathered about the Report. Further investigation will be carried out if the information and elements gathered are sufficient for the Report to be closed.

Prohibited reporting

The Whistleblower Manager will communicate this circumstance to the competent function for the possible commencement of disciplinary proceedings and the assessment of the Whistleblower's communication to the Whistleblower, in order to allow him/her to exercise his/her rights of defence. Should the competent function decide not to involve the reported person, the report received will be filed.
The involvement of other functions may also be required at a later stage if the defamatory, slanderous or discriminatory nature only emerges during the subsequent investigation phase.
It is forbidden, in any case:

- the use of insulting expressions
- sending Reports for purely defamatory or slanderous purposes
- sending Reports that relate exclusively to aspects of private life, without any direct or indirect connection with the reported person's business/professional activity
- sending Reports of a discriminatory nature, insofar as they refer to sexual, religious or political orientation or to the racial or ethnic origin of the reported person
- the sending of Reports made for the sole purpose of harming the reported person.

Such conduct, together with the sending of prohibited Reports or in any case made with wilful misconduct or gross negligence or deemed to be manifestly unfounded, shall be punishable in accordance with the disciplinary system adopted.
Possible sanctions are foreseen in the event of Reports made with wilful misconduct or gross negligence, or which prove to be false, unfounded, defamatory or otherwise made for the sole purpose of harming the Company, the reported person or other persons concerned by the Report.
It is specified that in cases of sending prohibited Reports, the confidentiality of the reporter's identity as well as the other measures for the protection of the reporter provided by the Company will not be guaranteed.

3. Report sent to a channel other than the one competent to receive it

Your confidentiality as a Whistleblower is protected even if the Report is made by means other than those established in accordance with the Decree or reaches staff other than those authorised and competent to handle Reports, to whom, in any case, they must be transmitted without delay.
If the internal Report is submitted to a person other than the one identified and authorised, the Report must be forwarded, **within 7 (seven) days of its receipt**, to the competent person.
You will be notified of the transmission of the Report at the same time.

The Report may be submitted to the hierarchical superior, but such a Report cannot be considered as whistleblowing, and therefore, in that case, you will not benefit from the protections provided for.

4. Report made in person

If a Report is made in person, directly to the Reporting Manager, the Reporting Manager may open the Report form on his or her own initiative, entering all the information needed to process the Report.

04. Investigations.

As part of the management of the internal reporting channel, the Reporting Manager performs the following activities:

- give the Reporting Party an acknowledgement of receipt of the Report within 7 (seven) days from the date of receipt, possibly indicating, if it does not deal with the Report directly, which other function will take charge of the Report, as the new Reporting Manager;
- maintains contacts with the reporter and requests additions if necessary
- follows up on reports received;
- provides feedback to the Reporting Party, on how the Report has been or is being handled, within 3 (three) months from the date of the acknowledgement of receipt or, in the absence of such notice, within 3 (three) months from the expiry of the 7 (seven) days from the submission of the Report. If the time needed for the investigation should be longer, at most every three months, a reply should be provided to the Reporting Party, explaining the circumstances that required the delay.

Once the case is ascertained and all the necessary measures put in place, the Reporting Manager closes the Report by acknowledging it to the Whistleblower through the Platform. All this is described in more detail in the following paragraphs.

1. Receipt of Report

When an Alert is received, regardless of the channel used, the Reporting Manager will assign a progressive identification number allowing it to be uniquely identified.

2. Preliminary analysis and evaluation

The Reporting Manager promptly takes charge of and analyses the Report received, with a view to its preliminary assessment.
Following this analysis, the Reporting Manager will classify the Report into one of the categories indicated in paragraph 3.2 above, which will imply a different and specific flow, possibly indicating the different function that will take charge of the operational management of the Report.

3. Investigations

At the end of the preliminary assessment phase, if the Report received is classified as 'material and treatable', the Reporting Manager will proceed with the initiation of internal checks and investigations in order to gather further detailed information to verify the merits of the reported facts and gather adequate evidence.
In the course of its investigative activities, the Reporting Manager may avail itself of the support of suitably qualified internal corporate structures and/or functions and/or through the use of external consultants.
In such circumstances, the persons involved in the investigation activity also become addressees of this Policy and are consequently called upon to comply with, inter alia, confidentiality obligations.
In the event of violations by such persons of the principles defined in this Policy, the Company may apply the measures indicated in the Model 231 sanctions system.

4. Verification Activity Report

The verification phase ends with the drafting of a report to formalise the context of the Report, the verification activities carried out, the methods followed and the results obtained.
The report will also propose actions to be taken in relation to each finding.

5. Conclusions

At the end of the investigation, if the Reporting Manager does not find that the unlawful conduct described in the Report is justified, or that such conduct does not constitute a Breach as defined in this Policy, he shall close the Report.
If, on the other hand, it deems it to be justified and the Report concerns employees of the Company, it shall promptly send the final report of the investigation to the Managing Director and to any other function deemed appropriate for the assessment of any disciplinary measures to be taken and/or for any communications to the competent Authorities.
At the same time, the Reporting Manager will consider informing the Board of Directors and the Board of Auditors.

6. Processing of personal data

It should be noted that the personal data of the Reporting Party, the Reporting Person and the Reported Person (the latter being regarded as 'data subjects' within the meaning of Article 4 GDPR) are processed in accordance with the GDPR and the Privacy Code.
In particular:

- processing activities related to the management of the Report are carried out in compliance with the principles laid down in Articles 5 (Principles applicable to the processing of personal data), 25 (Data protection by design and protection by default) and 35 (Data protection impact assessment) of the GDPR;
- before sending the Report, the Whistleblower receives the privacy notice pursuant to the GDPR, which provides information on the purposes and methods of the processing of his personal data, the duration of storage, the categories of recipients to whom the data may be disclosed in the context of the management of the Report, and the rights recognised to the Whistleblower by the GDPR. The Whistleblower is also provided with the privacy policy in accordance with the GDPR, also considering the risk of seriously compromising or making impossible the achievement of the processing purposes related to the Whistleblowing Procedure;
- the legal basis for the processing is the fulfilment of a legal obligation to which the Company is subject under the Decree;
- personal data will be processed within the European Economic Area (EEA) and stored on servers located within the EEA. However, the use of the WB Platform may result in access to the same by parties established in countries that do not belong to the European Union (EU) or the EEA. Such access, which may constitute an extra-EEA transfer, in any case, is carried out in compliance with the provisions of Chapter V of the GDPR;
- As indicated in the privacy policy provided to data subjects, personal data are processed for the time necessary to achieve the purposes justifying their collection and processing (e.g. collection and management of the Report) and are subsequently deleted or anonymised in accordance with the established retention periods;
- Appropriate technical (e.g. encryption within the WB Platform) and organisational measures are taken to ensure the security of personal data, in accordance with current legislation, both during the transmission of the Report and during its analysis, management and storage;
- the exercise of rights by the Whistleblower or the Reported Person in respect of his or her personal data processed in the context of the whistleblowing process is excluded pursuant to

Article 2-undecies of the Privacy Code in the event that such exercise may result in an actual and concrete prejudice to the 'confidentiality of the identity of the person reporting violations of which he or she has become aware by reason of his or her employment relationship'.

Access to the personal data of Reports is only granted to the Report Manager already authorised under the GDPR, limiting the disclosure of confidential information and personal data to third parties only when necessary.

7. Retention of alerts and related documentation

The Reports and the related documentation are kept for the time necessary for the processing of the Report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure , or until the conclusion of the judicial or disciplinary proceedings that may have been achieved against the Reported Person or the Reporting Person , in compliance with the confidentiality obligations set out in Article 12 of the Decree and the principle set out in Article 5(1)(e) of the GDPR (limitation of storage) and Article 3(1)(e) of Legislative Decree Legislative Decree No. 51 of 2018.

05. Rights and Duties of a Whistleblower

1. Confidentiality

The Company guarantees the confidentiality of the identity of the Whistleblower, the Whistleblower, the content of the Report and the documentation transmitted.
No retaliation or discrimination, direct or indirect, may result if you have made a Report in good faith. Furthermore, sanctions are provided for those who violate the measures for your protection as a Whistleblower.
Confidentiality is also guaranteed:

- any other information or element of the report from which your identity as a Whistleblower could be directly or indirectly deduced.
- in the case of reports - internal or external - made orally through voice messages, or through a direct meeting with the person dealing with the report.

Confidentiality is also protected:

- of the person reported;
- of the Facilitator both with regard to identity and to the activity in which the assistance takes place;
- persons other than the person reported but nevertheless implicated because they are mentioned in the Report (e.g. persons mentioned as witnesses).

The Company may also take appropriate action in court.

2. Judicial protection of the whistleblower

Your confidentiality as a Whistleblower is also guaranteed in the courts:

- within the framework of criminal proceedings, the identity of the reporter is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.
- within the framework of proceedings before the Court of Auditors, the identity of the reporter cannot be disclosed until the investigation phase is closed.
- within the framework of the disciplinary proceedings, the identity of the Whistleblower cannot be disclosed, if the allegation of the disciplinary charge is based on investigations other than the Whistleblowing, even if consequent to the Whistleblowing. If the charge is based, in whole or in part, on the Report, and it is essential for the accused's defence to know the identity of the Reporting Officer, the Report can be used for the purposes of the disciplinary proceedings only with the express consent of the Reporting Officer.

3. Express consent of the whistleblower

As stated above, in order to reveal your identity as a reporter, there must be:

- written communication of the reasons for the need to disclose the identity of the reporter, and
- the express consent of the reporting person.

The first scenario occurs when, in the context of a disciplinary procedure initiated against the alleged perpetrator of the reported conduct, your identity as a Whistleblower is indispensable for the defence of the person charged with the disciplinary offence.
In that case, in addition to your prior consent, the legislation also requires that you be informed, in advance and in writing, of the reasons justifying the disclosure of your identity.
The second hypothesis occurs, on the other hand, if the disclosure of your identity as a Whistleblower is also indispensable for the defence of the person concerned.
Again, in order to disclose your identity as a Whistleblower, it is necessary to obtain your consent in

advance and to notify you in writing of the reasons for the need to disclose your identity.

4. Protection from retaliation

All Whistleblowers, as also identified in paragraph 5 above, are protected against any form of retaliation. The protection applies not only if the Whistleblowing, whistleblowing or public disclosure occurs during the existence of the employment relationship, but also during the probationary period and before, or after, the termination of the employment relationship.
These are examples of prohibited retaliation (see definition above):

- dismissal, suspension or equivalent measures;
- relegation in grade or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion on improper lists on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of the contract for the supply of goods or services;
- cancellation of a licence or permit;
- the request to undergo psychiatric or medical examinations.

Protection from retaliation is also guaranteed:

- the facilitator (a natural person assisting the reporter in the reporting process and operating within the same work context);
- persons in the same employment context as the Whistleblower, the person making a complaint or the person making a public disclosure and who are linked to them by a stable emotional or family relationship up to the fourth degree;
- to work colleagues of the Whistleblower or of the person who has made a complaint or made a public disclosure, who work in the same work environment as the Whistleblower and who have a regular and current relationship with the Whistleblower;
- entities owned by the reporting person or for which those persons work, as well as entities operating in the same work environment as those persons.

The protection also extends to maintaining the confidentiality of those individuals.

To enjoy protection, it is necessary that

- the Whistleblower has reported on the basis of a reasonable belief that the information on the violations reported, disclosed or reported, is true and falls within the objective scope of the Whistleblowing Decree;
- the Report is made in accordance with the provisions of the Whistleblowing Decree and this Policy;
- there is a consequential relationship between the Report and the retaliatory measures suffered.

In any case, the protection envisaged in the event of retaliation is not guaranteed when the criminal

liability of the Whistleblower for the offences of defamation or slander or, in any case, for the same offences committed with the report to the judicial or accounting authorities, or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance. If liability is established, a disciplinary sanction is also imposed on the Whistleblower. Alleged retaliation, even if only attempted or threatened, must be reported exclusively to ANAC.

The Company prohibits any form of retaliation against those who make reports in good faith. Employees who make reports will not be subject to dismissal, threats, bullying, discrimination or any other form of retaliation. Any individual who retaliates against a whistleblower will be subject to disciplinary action, including the possibility of dismissal.

5. Support Measures

A list of third sector entities providing support measures to whistleblowers is established at ANAC.
The support measures provided consist of information, assistance and advice free of charge on how to report and on the protection from retaliation offered by national and EU legislation, on the rights of the person concerned and on the terms and conditions of access to legal aid.

6. Whistleblower responsibilities

The criminal and disciplinary liability of the Whistleblower in the event of a false, slanderous or defamatory report under the Criminal Code remains valid.
Any abuse of this procedure, such as reports that are manifestly opportunistic and/or made for the sole purpose of harming the whistleblower or other persons, and any other case of improper use or intentional exploitation of the institution covered by this Policy, shall also give rise to liability in disciplinary and other competent fora.
The overall investigation process from receipt of a report until the result of the investigation is shown below:

06. External reporting channels.

1. ANAC's external reporting channels

In cases where the Report relates to Breaches of European Union rules as referred to in (ii), (iii), (iv), and (v) of Chapter 1 above What may be reported and one of the following conditions is met

- when no internal reporting channel has been established or when the same, even if provided for, is not active;
- when the internal channel adopted does not comply with the provisions of Article 4 of the Decree;
- when the Signalling carried out by internal channel has not been followed up;
- when the Whistleblower has well-founded reasons - based on the particular circumstances of the case, precise and concordant - to believe that, if he/she were to make a Report through internal channels, it would not be effectively followed up or that the same Report might give rise to the risk of retaliation;
- when the Whistleblower has reasonable grounds - based on the particular circumstances of the case, precise and concordant - to believe that the breach may constitute an imminent or obvious danger to the public interest,

the Reporting Party may make a so-called external Report, through one of the channels made available by ANAC, which guarantee, also through the use of encryption tools, the confidentiality of the identity of the Reporting Party, of the Reported Subject, as well as of the content of the Report and of the relevant documentation.
External Reports may be made in writing via the IT platform or orally via telephone lines or voice messaging systems or, at the request of the Reporting Party, by means of a face-to-face meeting set within a reasonable time.
An External Report submitted to a person other than the ANAC is transmitted to the latter, within 7 (seven) days from the date of its receipt, with simultaneous notification of the transmission to the Reporting person.

2. Public disclosure

In cases where the Alert relates to Breaches of European Union rules as referred to in (ii), (iii), (iv), and (v) of Chapter 1 above What can be reported , and when one of the following conditions is met:

- the Whistleblower has previously made a Report through the Internal and External Channels, or has made an External Report directly, and in all these cases no response was given within the deadline;
- the Whistleblower has well-founded and reasonable grounds - on the basis of the particular circumstances of the case, which are serious, precise and concordant - to believe that the breach may constitute an imminent or obvious danger to the public interest (e.g. an emergency situation or the risk of irreversible damage, including to the physical safety of one or more persons, which require that the breach be promptly disclosed and have a wide resonance to prevent its effects);
- the Whistleblower has justified and reasonable grounds - on the basis of the particular circumstances of the case, which are serious, precise and concordant - to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the Whistleblower may be colluding with the author of the breach or involved in the breach itself,

the Reporting Party may make a Public Disclosure, through the press or electronic media or means of dissemination capable of reaching a large number of people

07. Sanctions.

It is recalled that any failure to comply with the provisions of this procedure may result in the imposition of disciplinary sanctions, in the cases provided for by law.
In this regard, it is clarified that the Company may impose disciplinary sanctions, as provided for in the Company's Sanctions System also adopted pursuant to Legislative Decree 231/01 as part of the Organisational Model and the applicable National Collective Labour Agreement, on those who

- retaliate against the Whistleblower, obstruct or attempt to obstruct Reports, breach confidentiality obligations as described above;
- have not carried out the verification and analysis of the Reports received.