



pq13 Illustration report management and whistleblowing protection

Scope of application: Dolomite Franchi SpA

Index:

- 1 OBJECTIVE**
- 2 FIELD OF APPLICATION**
- 3 RESPONSIBILITY**
- 4 PROCEDURE**
- 5 LABOUR PROTECTION**
- 6 ENVIRONMENTAL PROTECTION**
- 7 DOCUMENTATION/RECORDS**

1 Objective

This procedure is adopted by the Company in compliance with the provisions of Legislative Decree no. 24 of 10 March 2023 (in the text: Decree or D. Lgs. 24/2023) in force since 30 March 2023, which transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, concerning the protection of persons who report breaches of national or European Union law (the so-called whistleblowing directive) which come to their attention in the context of their work, detrimental to the public interest or the integrity of the public administration or private entity (i.e. Dolomite Franchi).d. whistleblowing directive) of which they become aware in the context of their work, detrimental to the public interest or the integrity of the public administration or private entity (i.e. Dolomite Franks).

2 Field of use

This procedure applies to any report of information on violations (as better specified in paragraph 4) acquired within the working context¹, if detrimental to the public interest or the integrity of the public administration or the private entity, made through the appropriate reporting channels made available by the Company.

They are excluded from the scope of this procedure:

- disputes, claims or demands of a personal nature that relate exclusively to individual employment relationships, i.e. employment relationships with hierarchically superior persons;
- national security breaches, as well as procurement relating to defence or national security aspects;
- violations mandatorily regulated by European Union or national acts² that already ensure appropriate reporting procedures.

2.1 References

- Legislative Decree No. 24 of 10 March 2023;
- Directive (EU) 2019/1937;

¹ To be understood as a subordinate employment relationship with the organisation or a professional/employment relationship, present or past.

² Please refer to the annexes of Directive 2019/1937 and Legislative Decree 24/23.

Title: pq13 Illustration report management and whistleblowing protection		
Nr.: pq13	Page 1 of 12	Rev:001/12.2023 Status: active



- Organisation, management and control model pursuant to Legislative Decree 231/01 and Dolomite Franchi's Code of Ethics;
- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree 196/2003 and ss.mm.ii.);
- ANAC Guidelines on the Protection of Persons Reporting Violations of Union Law and the Protection of Persons Reporting Violations of National Law Provisions - Procedures for the Submission and Management of External Reports approved by ANAC with Resolution No. 311 of 12 July 2023.

3 Responsibility

The Channel Manager, also through the use of the Whistleblowing platform:

- makes available, also through this procedure and the information published on the platform, clear information on the channel, procedures and prerequisites for internal reporting;
- issues the reporting person with an acknowledgement of receipt of the report within the deadline;
- assesses the criteria for processability of the report;
- diligently follows up on reports received;
- share the report with the Supervisory Board, the initiation of any investigations, their outcome and feedback to the reporter;
- sends feedback to the reporter on the closure of the handling of the report;
- maintains interlocutions with the reporting person and may request additions from the latter if necessary;
- files and stores the reporting documentation within the regulatory timeframe;
- ensures respect for the principle of confidentiality.

The Supervisory Board:

- follows up any information/report received by the person in charge of the channel, instructing him/her in accordance with Legislative Decree no. 231/2001 and the 231 Organisational Model in force if the reports concern, even if only potentially, the predicate offences referred to in Legislative Decree no. 231/2001 or violations of the 231 Organisational Model or the Code of Ethics adopted by the Company;
- ensures respect for the principle of confidentiality.

The Legal Representative of the Company:

- liaises with ANAC in the event of any external reporting or activation of inspection activities by ANAC.

The CDA:

- ensures that any measures are taken in accordance with the provisions of the sanctions system set out in the 231 Organisational Model;
- approves this procedure together with the associated organisational role structure;
- ensures compliance with the measures for the protection of the reporting person.

The Signalman:

- transmits reports in accordance with this procedure;
- is obliged to provide circumstantial information on the matter reported.

Those who, acting within the working environment of Dolomite Franchi, fall into the following categories will be protected under Legislative Decree 24/2023

- employees;



- self-employed workers and collaborators working for Dolomite Franchi
- freelancers;
- volunteers;
- consultants;
- shareholders;
- Providers of services for third parties in any capacity whatsoever (irrespective of the nature of such activities) even without consideration;
- even unpaid trainees;
- persons exercising functions of administration, management, control, supervision or representation, even if the relevant activities are performed in a de facto and not in a de jure capacity.

Also included in this category are all those persons who, for whatever reason, become aware of offences in the context of the Company's working environment, i.e:

- when the employment relationship has not yet begun;
- during the probationary period;
- upon termination of the relationship.

4 Procedure

4.1 Definitions³

- **'Reports'** means any written or oral communication set out in an interview, even in anonymous form, containing information on violations;
- **"violations"**: conduct, acts or omissions that harm the public interest or the integrity of the private entity (i.e. Dolomite Franchi) and that consist of:
 - a) **unlawful conduct pursuant to Legislative Decree No. 231/2001** or violations of the Company's **Organisation, Management and Control Model**;
 - b) **offences falling within the scope of application of the European Union or national acts indicated in the annex to Legislative Decree no. 24/2023** or of the national acts constituting implementation of the European Union acts indicated in the annex to EU Directive no. 1937/2019, even if not indicated in Legislative Decree no. 24/2023, 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 protection of personal data and security of networks and information systems (List of European and national regulations mentioned in Legislative Decree No. 24/2023, Annex a);
 - c) **acts or omissions affecting the financial interests of the Union**;
 - d) **acts or omissions affecting the internal market**, including violations of EU competition and State aid rules, as well as violations affecting the internal market related to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
 - e) **acts or conduct that frustrate the object or purpose of the provisions of Union acts in the areas referred to in (b), (c) and (d) above.**
- **"Information on breaches"** means all information, including reasonable suspicions, concerning breaches committed or likely to be committed in the organisation with which the reporting person or the person making the complaint to the judicial/accounting authority has

³ Some of the definitions therein refer to the provisions of Article 2 of Legislative Decree 24/2023 to which reference is made for the full version.



a legal relationship and also information concerning conduct aimed at concealing such breaches;

- **"internal reporting"**: communication of "reports" through the established internal reporting channel;
- **"External reporting"** means the written or oral communication of information on violations, submitted through the external reporting channel⁴ ;
- **"public disclosure"** means making information about infringements publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people;
- **'Whistleblower': an individual who makes a report** or public disclosure of information about violations acquired in the context of his or her work;
- **'Facilitator': a natural person** who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- **'employment context' means** present or past work or professional activities through which, regardless of the nature of such activities, a person acquires information about violations and in the context of which he or she could risk retaliation in the event of a public report or disclosure to the judicial or accounting authorities;
- **"Person involved" means the** natural or legal person mentioned in the report as the person to whom the breach is attributed or as a person otherwise implicated in the reported breach;
- **"channel manager"**: an external person identified by the Company responsible for channel management and reporting with organisational and functional autonomy;
- **"Retaliation"**: any conduct, act or omission, even if only attempted or threatened, occurring as a result of the whistleblowing and closely related to the whistleblowing, the report to the judicial or accounting authorities or the public disclosure and which causes or may cause the whistleblower or the person who made the report, directly or indirectly, unjust damage;
- **"Follow-up" means the** action(s) initiated by the entity entrusted with the management of the reporting channel;
- **"Acknowledgement" means the** communication to the person making the alert of information on the action taken or intended to be taken on the alert, including the measures envisaged or to be taken and the reasons for the choice made;
- **"platform": an internal reporting channel** adopted by the Company (as further specified in section 4.2) to transmit information on violations;
- **"Supervisory Board ("SB")"**: Supervisory Board pursuant to Legislative Decree 231/2001;
- **"Model 231"**: Organisation, management and control model pursuant to Legislative Decree 231/2001.

4.2 Internal signalling channel

The Company has provided for an internal reporting channel to be used by whistleblowers for the transmission of information on violations. The use of this channel allows for more effective prevention and detection of violations. This choice responds to the principle of fostering a culture of good communication and corporate social responsibility, as well as improving its organisation.

Warning: Reports concerning breaches of Legislative Decree No. 231/2001 and of the relevant Organisation and Management Model may only be made through the internal channel.

The internal reporting channel provides for written or oral reporting through the Whistleblowing Reporting platform accessible at the link whistleblowing-dolomitefranchi.digimog.it.

Internal reports in oral form are made, at the request of the reporting person via the platform itself, by means of a face-to-face meeting set within a reasonable time at an agreed protected location.

⁴ see Art. 7 of Legislative Decree 24/2023.



The internal reporting channel guarantees the confidentiality of the identity of the reporter, the facilitator (if any), the persons involved and in any case mentioned in the report, as well as the content of the report and of the relevant documentation submitted or that can be supplemented.

4.2.1 Person responsible for the management of the internal channel (so-called 'Channel Manager')

Dolomite Franchi has decided to entrust the management of the internal reporting channel to the members of the Company's Supervisory Board, specifically appointed, in possession of the requirements of autonomy, independence and specifically trained.

The person in charge of managing the channel and reporting acts exclusively with regard to the acquisition of the report and access to the platform.

For any Reports of facts in which the Supervisory Board is directly involved, its attributions, competences and powers are transferred to the Board of Auditors, which handles such Reports in compliance with this procedure.

4.2.2 Characteristics of the internal signalling channel

The Company's internal whistleblowing channel is supported by the 'Whistleblowing Reporting' platform, is web-based and accessible from all devices (PC, Tablet, Smartphone).

Data entered into the platform are segregated in the logical partition dedicated to the company and subjected to a scripting algorithm before being stored. Security in transport is guaranteed by secure communication protocols.

At the end of the submission of the report (whether anonymous or not), the platform provides a 16-character alphanumeric code, randomly and automatically generated by the platform, which cannot be reproduced, and with which the reporter can at any time view the processing status of his report and interact with the person responsible through a messaging tool.

The report can only be viewed and managed by authorised persons. The person responsible has unique credentials for access, expiring every 6 months. The password policy adheres to international best practices. The platform sends reminders about unread or out-of-date reports to the channel manager.

The retention period for reports is envisaged to be no longer than five years from the date of communication of the final outcome of the reporting procedure; on expiry, the platform automatically proceeds to delete the data. This is without prejudice to the possibility of defending the rights of the data controller in all venues, in particular in the event of any legal proceedings.

The processing of personal data must always take into account and comply with the obligations set out in the GDPR and Legislative Decree 196/2003. Dolomite Franchi, as data controller through the internal reporting channel, has carried out a prior analysis of the organisational design including an assessment of the possible impact on data protection (Art. 35 GDPR).

4.2.3 Characteristics of reporting and anonymous reporting

It is necessary that the report be as detailed as possible in order to allow the analysis of the facts by the persons competent to receive and handle reports. In particular, it must be clear:

- the circumstances of time and place in which the reported event occurred;
- description of the fact;
- personal details or other elements enabling identification of the person to whom the reported facts can be attributed.

Information on reported violations must be truthful. Mere suppositions, unreliable indiscretions (so-called rumours), as well as news in the public domain, incorrect information (with the exception of genuine error), manifestly unfounded or misleading, or if merely damaging or



offensive, are not considered such. On the other hand, it is not necessary for the reporter to be certain of the actual occurrence of the reported facts and the identity of the author thereof.

It is also useful for the whistleblower to provide documents that may provide evidence of the facts being reported, as well as an indication of other persons potentially aware of the facts.

Anonymous reports, where substantiated, are equated with ordinary reports and in that case considered within the scope of this procedure also with regard to the protection of the reporter, if subsequently identified, and to record-keeping obligations.

4.2.4 Operational procedure for handling the report

The reporter transmits the alert via the dedicated internal channel.

The whistleblower activates the report in written mode, by filling in a guided form via the above-mentioned link, or in oral mode by requesting a meeting with the Channel Manager via the above-mentioned platform.

If the reporting person makes the report orally by means of a fixed meeting with the person in charge of the channel, the report, subject to the consent of the reporting person, is documented by the person in charge of the channel by means of a record that the reporting person may verify, rectify and/or confirm by signing.

Receipt of the report by the person in charge of the channel initiates the report handling process. The person in charge of the channel proceeds to process it according to a predefined process flow chart.

Upon receipt of the report, the platform automatically notifies the reporting party of the receipt of the report, thereby fulfilling the obligation to send an acknowledgement of receipt to the reporting party within 7 days of receipt of the report, as provided for in Legislative Decree 24/2023.

The platform sends reminders to the channel manager of unread or out-of-date reports.

The person in charge of handling the report proceeds with an initial check on the correctness of the procedure followed by the reporting party and the content of the report, both with reference to the scope defined by this procedure (so-called inherent nature of the report content) and to its verifiability on the basis of the information provided. The person in charge of the channel, having ascertained the inherent nature of the report and having acquired all the elements, in compliance with the principle of confidentiality, also acts in the capacity of Supervisory Body in the event of relevance under Legislative Decree no. 231/01 of the report, in order to assess the modality of initiating the investigation phase, without prejudice to the respect of the principle of autonomy and independence of the aforementioned persons with respect to the manner in which they handle the report.

If the report does not relate to violations as defined in paragraph 4.1, the channel manager formalises the outcome of the check and communicates it to the reporter within a reasonable timeframe (no more than three months) and files the report. The person in charge, guaranteeing respect for the principle of confidentiality, shares the report with the Company.

If additional information is needed, the channel manager will contact the reporter via the platform. If the whistleblower does not provide additional information within 3 months of the request for supplementation, the channel manager will proceed with the archiving of the report and notify the whistleblower accordingly. If it is necessary to transfer data outside the platform, in particular personal data of the whistleblower, the Channel Manager requests the whistleblower's explicit consent via the platform.

Acknowledgement of receipt of the report must be sent to the reporter within three months from the date of receipt of the report. Only in exceptional cases, should the complexity of the report so require, or in view of the reporting party's response time, the person in charge of the channel,



having promptly informed the reporting party before the deadline, with appropriate justification, may continue the investigation phase for as long as necessary and giving the reporting party regular updates.

The Supervisory Body, within the scope of its operational autonomy, assesses, if the report is well-founded, any consequent measures and adopts any measures deemed necessary for the purposes of adapting the Model, taking the necessary communications for the application of any sanctions. Any consequent measures are applied in accordance with the provisions of the disciplinary system set out in the 231 Organisational Model.

For reports that do not fall within the perimeter of violations pursuant to Legislative Decree No. 231/01, the person in charge of the channel will assess, on a case-by-case basis, with the Company whether and which corporate function should be appropriately involved for the relevant analysis and any consequent measures, always in compliance with the principle of confidentiality.

In the event that the report proves to be in fact an act of defamation or slander, ascertained by a conviction, even at first instance, the Company shall proceed with disciplinary proceedings against the reporter.

It is specified that, from receipt of the report until its closure, any person in a situation of conflict of interest must refrain from taking decisions in order to ensure compliance with the principle of impartiality.

4.2.5 Transmission of alerts with wrong addressee

If the report is transmitted to a person other than the person responsible for receiving it, the person receiving it is obliged to transmit it within seven days to the competent person, giving notice of the transmission to the reporting person and guaranteeing a chain of custody of the information that complies with confidentiality obligations and with those set out in paragraph 7.2. The Company adopts disciplinary sanctions in the event of non-compliance with the transmission obligation.

In the case of inadvertent transmission of the report to a person other than the person entitled to receive it, the reporter must prove mere negligence and the absence of a personal interest in the erroneous transmission.

4.2.6 Retention of documentation on internal reporting

Internal reports and all accompanying or supplemented documentation are retained, with an appropriate digital chain of custody, for as long as the report itself is processed.

In any case, the documentation shall only be kept for a period of up to five years from the date of the communication of the final outcome of the alert procedure.

In all the cases mentioned, the procedure for keeping internal reports and related documentation must comply with EU and national guarantees on the processing of personal data as well as with the measures in place on the right to privacy.

4.2.7 Information obligations

Information on the channel, procedures and prerequisites for making reports is displayed in workplaces, on the Company's Intranet, and made known to persons who, although not attending workplaces, have a legal relationship with the Company through publication on the Company's website.

The Company activates its internal reporting channel after hearing the representatives or trade union organisations.



4.3 External signalling

Only for breaches that concern offences falling within the scope of the European Union or national acts indicated above - para. 4, letters b), c), d), e) - it is possible for the reporter to make an external report through the channel activated at the ANAC (National Anti-Corruption Authority) (the external reporting channel cannot be activated for reports concerning breaches of Legislative Decree no. 231/2001 and breaches of the Organisation and Management Model).

However, it should be noted that only if the following conditions are met, the reporter may proceed with a report to ANAC through an external channel:

- a) if in the relevant work context, activation of the internal reporting channel is not mandatory or the channel itself has not been activated or does not comply with regulatory requirements;
- b) when the reporter has already submitted an internal report even though it has not been followed up;
- c) if the whistleblower has a well-founded reason to believe that by submitting an internal report, the report will not be effectively followed up or that the report, in itself, will lead to retaliation against him/her;
- d) where the reporter has a well-founded reason to believe that the reported breach may constitute an imminent or obvious danger to the public interest.

The external body entitled to receive external reports is ANAC in accordance with the appropriately adopted modalities and procedures (<https://www.anticorruzione.it/-/whistleblowing>).

The existence of the conditions for using the external reporting channel must be adequately justified by the Whistleblower; in particular:

- a report "*has not been acted upon*" (see (b) above) when it has remained totally unreported;
- *the "well-founded reasons"* referred to in (c) and (d) above must be objective and adequately substantiated.

4.4 Public Disclosure

On a residual and subordinate basis, the reporter may proceed with a public disclosure in the following cases:

- a) when it has already previously made an internal or external report, or has directly made an external report without having received a reply within the prescribed time limit;
- b) where it has reasonable grounds to believe that the breach constitutes an imminent or obvious danger to the public interest;
- c) where it has reasonable grounds to believe that the external report carries the risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may be in collusion with the infringer or involved in the infringement.

As regards the definition of '*well-founded reason*', see the section entitled 'EXTERNAL NOTIFICATION'.

Attention: *the external reporting channel and public disclosure cannot be activated in the event of unlawful conduct relevant under Legislative Decree No. 231/2001 or violations of the Organisation and Management Model or the Company's Code of Ethics.*



4.5 Duty of Confidentiality

All alerts and their annexes shall not be used beyond the time required to follow them up.

It is provided that the identity of the reporter together with any other information from which it may be inferred, directly or indirectly, shall not be disclosed without the express consent of the reporter himself/herself to persons other than those competent to receive or follow up the reports, expressly authorised to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2-quaterdecies of the Personal Data Protection Code set out in Legislative Decree No. 196 of 30 June 2003.

The Company shall protect the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated on account of the report, in compliance with the same guarantees provided for in favour of the reporting person.

Mitigating circumstances for the protection of the right to privacy include:

- In the context 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: the obligation of secrecy is imposed on the acts of the preliminary investigation until such time as the suspect has the right to have knowledge of them and, in any case, no later than the closure of that phase;
- Within the framework of the proceedings established at the Court of Auditors, the identity of the reporter cannot be disclosed until the investigation phase is closed;
- within the framework of disciplinary proceedings, the identity of the whistleblower may not be disclosed where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it;
- where the accusation is based, in whole or in part, on the report and knowledge of the identity of the person making the report is indispensable for the accused's defence, the report will only be usable for the purposes of disciplinary proceedings if the person making the report expressly agrees to reveal his identity;
- in cases of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, written notice shall be given to the reporter of the reasons for disclosing confidential data when disclosure is also indispensable for the defence of the person concerned.

Subject to the mitigation measures listed above, the affected party, upon its request, is also heard through a cartel procedure by means of the acquisition of written observations and documents.

Confidentiality obligations include:

- the subtraction of the report and of the documentation attached thereto from the right of access to administrative acts provided for by Articles 22 et seq. of Law No. 241/1990 and to generalised civic access pursuant to Articles 5 et seq. of Legislative Decree No. 33/2013;
- The administrations and bodies involved in the handling of reports guarantee confidentiality during all stages of the reporting process, including the possible transfer of reports to other competent authorities.

4.6 Protection of personal data

All processing of personal data, including communication between the competent authorities, is carried out in accordance with the law:

- of Regulation (EU) 2016/679;



- of Legislative Decree no. 196 of 30 June 2003, as amended and supplemented.

The disclosure of personal data by EU institutions, bodies or entities is made in accordance with Regulation (EU) 2018/1725.

The processing of personal data relating to the receipt and handling of reports is carried out by the data controller, in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, by first providing appropriate information to the reporting subjects and the persons concerned and by taking appropriate measures to protect the rights and freedoms of the persons concerned.

The information to data subjects, which also summarises their rights and how to exercise them, is made available, with acknowledgement required, within the Whistleblowing Reporting application.

Where it is necessary to disclose the identity of the reporting person to persons other than those responsible for receiving and handling the report, in compliance with the provisions of Legislative Decree 24/2023, the reporting person will be asked for express and specific consent.

4.7 Protection and support measures

Appropriate measures are in place to protect whistleblowers from direct retaliation and indirect retaliation.

Protection measures apply if at the time of the report the reporting person had reasonable grounds to believe that the information on the reported violations was true (see Section 4.2.3), fell within the objective scope and the reporting procedure was followed.

In the event that the report turns out to be in fact an act of defamation or slander, established by conviction even in the first instance, protections are not guaranteed.

Protection measures also apply:

- a) to facilitators;
- b) persons in the same work environment as the reporting/reporting person who are related to them by a stable emotional or kinship link up to the fourth degree;
- c) co-workers of the reporting/whistleblowing person who work in the same work environment as the reporting/whistleblowing person and who have a regular and current relationship with that person;
- d) entities owned by the reporting/whistleblowing person or for which those persons work, as well as entities operating in the same work environment as those persons.

Attention: In any case, it is emphasised that **ONLY reports concerning 'violations' as defined above fall within the scope of this procedure and, therefore, the protections set out below will apply.**

It is understood that reports which are not considered relevant for the purposes of this procedure, and therefore outside the scope of application of Legislative Decree no. 24/2023, will be filed by the Reporting Manager as "non-whistleblowing reports" and forwarded to the competent Functions for them to carry out their own investigative activities

4.7.1 Prohibition of retaliation

The persons listed in paragraph 3 may not suffer any retaliation. For information purposes and not as an exhaustive list, "retaliation" shall be considered:

- dismissal, suspension or equivalent measures;
- relegation in grade or non-promotion;



- the change of functions;
- the change of workplace;
- salary reduction;
- the modification of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references that are not adequately substantiated;
- the adoption of disciplinary measures or other sanctions (including fines);
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination or otherwise unjustified 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,
- 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;
- the early termination or cancellation of a contract for the supply of goods or services;
- cancellation of a licence or permit;
- the request to undergo psychiatric or medical examinations.

Acts taken in violation of the prohibition of retaliation are null and void.

In the context of judicial or administrative proceedings, or in the case of out-of-court disputes concerning the ascertainment of the prohibited conduct, acts or omissions against the reporting person alone, it is presumed that such conduct or acts were carried out as a result of the reporting. The burden of proving that such conduct or acts are motivated by reasons unrelated to the reporting is on the person who carried out the retaliatory acts.

Whistleblowers may inform ANAC of retaliation they believe they have suffered, whether attempted or contemplated.

The ANAC informs the National Labour Inspectorate, for measures within its competence.

4.7.2 Support Measures

The reporting party may turn to Third Sector entities on the list published on the ANAC website. These are bodies which carry out activities of general interest for the pursuit, on a non-profit basis, of civic, solidarity and socially useful purposes ('promotion of the culture of legality, peace among peoples, non-violence and non-armed defence; promotion and protection of human, civil, social and political rights, as well as the rights of consumers and users of general interest activities; promotion of equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing groups') and which have entered into agreements with 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.

4.7.3 Limitation of liability of the reporter

There is no liability (including civil or administrative liability) for those who disclose or disseminate information on violations:

- covered by the obligation of secrecy,



- related to copyright protection,
- of the provisions on the protection of personal data,
- which offend the reputation of the person involved or denounced,

whether, at the time of the disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the breach and the reporting was consistent with the conditions for protection.

In addition, protective measures include:

- The rights to make a report and the related protections cannot be restricted in a contractual manner;
- the exclusion of all other liability, including civil and administrative liability, for the acquisition of or access to information on violations, unless the conduct constitutes a criminal offence;
- the exclusion of any other liability with regard to conduct, acts, omissions carried out if connected to the report and strictly necessary to disclose the violation or, in any case, not connected to the report.

4.8 Penalty regime

The disciplinary system adopted by Dolomite Franchi pursuant to Article 6, paragraph 2, letter e), of Legislative Decree 231/2001, provides for sanctions to be applied against those whom the Company ascertains to be responsible for offences relating to

- commission of retaliation or proposed adoption, obstruction of reporting (even attempted) or breach of confidentiality obligations,
- Failure to set up reporting channels, failure to adopt procedures for handling them, or procedures that do not comply with the requirements of the decree, or failure to verify and analyse reports,
- civil liability of the reporting person for defamation or slander in cases of wilful misconduct or gross negligence, unless that person has already been convicted, also at first instance, of the offences of defamation or slander;

as well as against anyone who violates this procedure.

5 Labour protection

-

6 Environmental Protection

-

7 Documentation/Records

- Information on the processing of personal data Whistleblowing