

## Index

1. INTRODUCTION	2
2. PURPOSE AND AIMS OF THE PROCEDURE	3
3. NORMATIVE REFERENCES	3
4. DEFINITIONS	3
5. WHISTLEBLOWERS	5
6. REPORTABLE VIOLATIONS	5
7. ANONYMOUS REPORTING	6
8. THE INTERNAL REPORTING CHANNEL	6
9. THE CONTENT OF THE ALERT	7
10. THE OPERATOR OF THE INTERNAL REPORTING CHANNEL	8
11. RECEIPT OF 'OUT-OF-CHANNEL' SIGNALLING	8
12. THE MANAGEMENT OF INTERNAL REPORTING	8
13. OBLIGATION OF CONFIDENTIALITY	10
14. PROCESSING OF PERSONAL DATA	11
15. KEEPING RECORDS OF ALERTS	11
16. THE WHISTLEBLOWER'S PROTECTION MEASURES	12
17. THE PROTECTION OF THE REPORTED PERSON	15
18. EXTERNAL REPORTING	15
19. PUBLIC DISCLOSURE	16
20. SANCTIONS	18
21. THE PUBLICITY OF THE PROCEDURE	18
22. AWARENESS-RAISING INITIATIVES	18
23. MODIFICATION OF MODEL 231 FOLLOWING REPORTS	18

## REVISION MATRIX

Revision	Date	DESCRIPTION OF THE MODIFICATION
00	14/09/2018	First issuance of the document
01	14/07/2023	Update pursuant to Legislative Decree 24/2023

Edited	Verified	Approved
<b>Avv. Yuri Nadelreich</b>	<b>Legal Department</b>	<b>Marco Valle (CEO)</b>

## 1. INTRODUCTION

*Whistleblowing* is an Anglo-Saxon-derived tool through which employees of an organisation, whether public or private, report to specific individuals or bodies a violation, crime or wrongdoing, committed by others in the organisation.

The term *whistleblowing* identifies 'the reporting of *violations*'.

The purpose of *whistleblowing* is to enable organisations to deal with the reported problem as soon as possible, by disclosing situations of risk or harm and contributing to the prevention and prosecution of any wrongdoing.

The virtuous management of *whistleblowing* contributes not only to detecting and combating possible wrongdoing and to spreading a culture of ethics and legality within organisations, but also to creating a climate of transparency and a sense of participation and belonging, generated by overcoming employees' fears of being retaliated by company bodies or colleagues, or the risk of seeing their reports unheeded.

On 26 November 2019, the European Union published the '*EU Whistleblower Protection Directive*'.

EU Directive 1937/2019 provided for the protection of *whistleblowers* within the Union, by means of minimum standards of protection, aimed at standardising national laws, taking into account that those who report threats or harm to the public interest that they have become aware of in the course of their professional activities exercise their right to freedom of expression.

On 15.03.2023, Legislative Decree No. 24 of 10 March 2023 "*implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws*" was signed.

In Italy, until the enactment of Legislative Decree No. 24/2023, the obligation to set up a *whistleblowing* system enabling the whistleblower to report violations was provided for in the public sector (introduced by art.1, paragraph 51, of Law 190/2012) and, in the private sector (introduced by Law No. 179 of 30 November 2017 which supplemented Article 6 of Legislative Decree 231/2001) exclusively (i) for companies with an organisational model pursuant to Legislative Decree 231/01, (ii) and for companies subject to the Consolidated Banking Act, the Consolidated Finance Act, anti-money laundering regulations and the Private Insurance Code.

With Legislative Decree No. 24/2023, the institute of *whistleblowing* was extended to all public entities, to private sector entities with an average of at least 50 employees in the last year, to private sector entities with an average of less than 50 employees in the last year if they operate in certain sectors, and to private entities with an organisational model pursuant to Legislative Decree 231/01, even if they have fewer than 50 employees.

This Decree expressly repeals the provisions of Article 54-bis of Legislative Decree No. 165 of 30 March 2001 and Article 6, paragraphs 2-ter and 2-quater of Legislative Decree No. 231 of 8 June 2011, and amends Article 6,

paragraph 2-bis of Legislative Decree No. 231 of 8 June 2011.

The Decree brings together in a single regulatory text the entire discipline of reporting channels and the protections afforded to whistleblowers in both the public and private sectors. The result is an organic and uniform discipline aimed at greater protection of the reporter; in this way, the latter is given a greater incentive to make reports of wrongdoing within the limits and in the manner indicated in the Decree.

## 2. PURPOSE AND AIM OF THE PROCEDURE

The purpose of this procedure of Azimut Benetti S.p.A. (hereinafter referred to as "**Azimut Benetti**") is to remove factors that may hinder or discourage recourse to the institute, such as doubts and uncertainties about the procedure to be followed and fears of retaliation or discrimination.

With this in mind, the purpose of this procedure is to:

- a) ensure the confidentiality of the identity of the whistleblower and the content of the report, as well as the prohibition of retaliation in the working relationship;
- b) provide the whistleblower with clear operational indications on the subject, content, addressee and modalities of transmission of the report, as well as on the forms of protection offered to him/her in our legal system;
- c) regulate the process of handling the report by the recipient of the report;
- d) provide the whistleblower with operational guidance on the conditions for making an external report.

The illustrative slides of this procedure are available in the dedicated section of the company intranet, as well as on the Azimut Benetti S.p.A. website.

## 3. NORMATIVE REFERENCES

- EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law;
- Legislative Decree 24/2023 implementing EU Directive 1937/2019 (hereinafter, for brevity, simply 'Decree');
- Legislative Decree No. 231/2001, concerning '*regulation of the administrative liability of legal persons, companies and associations, including those without legal personality*';
- European Data Protection Regulation 2016/679 (GDPR) and D. Lgs. 196/03.

## 4. DEFINITIONS

- "**violations**": conduct, acts or omissions detrimental to the public interest or the integrity of the public administration or the private entity referred to in Article 2, comma 1, lett. a, n. (1), (2), (3), (4), (5) and (6) of the Decree;

- **"information on violations"** means information, including reasonable suspicions, concerning violations committed or likely to be committed in the organisation with which the reporting person or the person making the complaint to the judicial or accounting authorities has a legal relationship, as well as elements concerning conduct aimed at concealing such violations;
- **'reporting'** means the written or oral communication of information on violations;
- **'internal reporting'** means the communication, written or oral, of information on violations, submitted through the internal reporting channel;
- **"external reporting"** means the communication, in writing or orally, of information on violations, submitted through the external reporting channel;
- **"public disclosure"** or **"public dissemination"** 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;
- **"manager of the internal reporting channel"**: the Supervisory Body of Azimut Benetti S.p.A.;
- **'whistleblower'** means the natural person who makes a report or public disclosure of information about violations acquired in the context of his or her work;
- **"reported person"** means any person to whom the facts that are the subject of a report are referred or referable;
- **'facilitator'**: a natural person who assists the reporter in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- **'employment context'** means the work or professional activities, present or past, through which, irrespective 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 disclosure or report to a judicial or accounting authority;
- **"person involved"** or **"reported"** means the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as a person otherwise implicated in the reported or publicly disclosed breach;
- **"retaliation"** shall mean any conduct, act or omission, even if only attempted or threatened, occurring as a result of the report, the complaint to the judicial or accounting authorities or public disclosure and which causes or may cause the whistleblower or the person who made the report, directly or indirectly, unjust damage;
- **"Follow-up"**: the action taken by the entity entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigation and any measures taken;
- **"Company"**: Azimut Benetti S.p.A.;

- **"feedback"** means the communication to the reporter of information concerning the follow-up given or intended to be given to the report.

## 5. THE WHISTLEBLOWER

The persons who may report are:

- 1) employees;
- 2) the self-employed and collaborators;
- 3) workers or collaborators of the Company's suppliers;
- 4) freelancers and consultants working for the Company;
- 5) volunteers and trainees, paid and unpaid, working for the Company;
- 6) shareholders and persons with administrative, management, control, supervisory or representative functions, even if such functions were exercised on a de facto basis.

Reporting can be done:

- in constancy of the working relationship;
- in the pre-contractual phase (thus also by the candidates);
- during the probationary period;
- after termination of the relationship, if the information was acquired during the course of the relationship.

## 6. REPORTABLE VIOLATIONS

The following violations may be reported:

- (1) administrative, accounting, civil or criminal wrongdoing, as well as unlawful conduct pursuant to Legislative Decree No. 231/2001 or violations of the organisation and management models provided for therein, which do not fall under numbers 2), 3), 4) and 5) below;
- (2) wrongdoing falling within the scope of European Union or national acts 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 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;
- (3) acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary law of the European Union;
- (4) acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including violations of European Union competition and State aid rules, as well as

violations relating to 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;

(5) acts or conduct that frustrate the object or purpose of the provisions of Union acts;

of which the whistleblower has become aware in the context of his or her work and which consist in conduct, acts or omissions detrimental to the integrity of the Company.

The following reports are not handled:

- reports concerning violations other than those described above;
- disputes, claims or requests linked to a personal interest of the whistleblower or the person lodging a complaint with the judicial or accounting authorities, which relate exclusively to his or her individual work or public employment relationships, or which are inherent to his or her work or public employment relationships with hierarchically superior figures.

## 7. ANONYMOUS REPORTING

An anonymous report, i.e. one that does not contain any elements allowing its author to be identified, shall be treated in the same way as an ordinary internal report and similarly handled in accordance with the provisions of this procedure. Nevertheless, also in consideration of the measures implemented to protect the whistleblower, the Company encourages the inclusion of the whistleblower's data in order to facilitate investigations.

## 8. THE INTERNAL REPORTING CHANNEL

Reports can be submitted via the My Governance platform <https://www.mygovernance.it/token-azimut/>, which is based on encryption at the source of the report, guaranteeing the integrity and non-violability of its content and allowing access only to the reporting manager (the Supervisory Body of Azimut Benetti S.p.A.).

The platform allows you to submit a report via the web either in written form, by filling in a form, or orally (from August 2023). It will also be possible to request a face-to-face meeting with the reporting manager (by indicating this on the screen where the description of the facts is requested), to be arranged within 7 days of the reporting party's request.

The system guarantees that the whistleblower will be automatically informed that the report has been taken care of and will be able to view the status of the report, interact with a messaging system with the receiver and thus be contacted in order to acquire useful elements for the investigation phase or to send further information that he/she may need in order to supplement the facts that are the subject of the report.

The reporting manager, notified by e-mail of each report received by the system, can access the list of reports, view their status, download the information sent, send messages with requests for further information to the whistleblower, and report the status of the report as closed.

The platform administrator cannot access the content of the reports.

The platform, through the management of data *retention* and *logging* policies, does not allow digital tracking of the reporter, thus guaranteeing the confidentiality of the whistleblower's identity.

The software underlying the platform is specifically designed with high-risk usage scenarios in mind and, for this reason, the main state-of-the-art security protocols are implemented with a preference for public domain protocols with the benefit of public *peer-review*: these include the use of the https protocol, which offers encryption of alerts and their attachments.

Messages are delivered to the reporting manager in encrypted form and can only be deciphered using a key held by the alert manager alone.

Any subsequent communication between the whistleblower and the reporting manager must take place within the platform, via the messaging service, and not through e-mail or other channels.

For more precise operating instructions on how to make a report, the My Governance vademecum is available in the dedicated section of the company intranet, as well as on the Azimut Benetti S.p.A. website.

## 9. THE CONTENT OF THE REPORT

The content of the report is free, but in order to facilitate investigations, the following elements should be included:

- the personal details of the whistleblower;
- a clear and complete description of the facts being reported;
- if known, the circumstances of time and place in which the reported facts were committed;
- if known, the personal details or other elements enabling the identification of the person(s) who has/have carried out the reported facts;
- an indication of any other persons who may report on the facts being reported;
- any documents that may confirm these facts;
- any other information that may provide useful feedback on the existence of the reported facts.

The report may also relate to information on conduct aimed at concealing the aforementioned violations or unlawful activities that have not yet been committed but which the whistleblower reasonably believes may occur in the presence of concrete, precise and concordant elements.

The report must be made in good faith and must not take an insulting tone or contain personal insults or moral judgments designed to offend or harm the personal and/or professional honour and/or decorum of the person or persons to whom the facts reported are allegedly ascribed. Where, on the basis of the assessments and investigations carried out, the facts reported turn out to be unfounded and/or inconsistent, the whistleblower who made the report in good faith shall not be prosecuted.

## 10. THE OPERATOR OF THE INTERNAL REPORTING CHANNEL

The management of the internal reporting channel is entrusted to the Supervisory Body (hereinafter also referred to as the "SB" or ) appointed by Azimut Benetti pursuant to Article 6 of Legislative Decree 231/01, which is required to perform the following tasks:

- a. ensure that the system for handling reports of violations is designed and resourced to ensure a comprehensive assessment of reports;
- b. ensure, that the investigation and protection functions are carried out independently;
- c. Provide advice and guidance on the reporting management system and on issues related to the reporting of violations;
- d. report on a planned basis on the progress of the reporting system to the Board of Directors.

## 11. THE RECEIPT OF THE 'OUT-OF-CHANNEL' REPORT

An internal report submitted to a person other than the reporting manager must be forwarded, within 7 (seven) days of its receipt, to the manager with simultaneous notice of the transmission to the reporting manager.

## 12. MANAGING INTERNAL REPORTING

The procedure for handling internal reports consists of the following steps:

- a. receiving and registering the report;
- b. preliminary assessment of the report;
- c. pre-trial phase;
- d. phase of communicating the outcome of the investigation.

### A) Receiving and registering the report

The procedure for handling reports is initiated upon receipt of the report.

Once the report has been submitted, the platform sends the whistleblower immediate confirmation of correct entry. Within 7 (seven) working days from that moment, the operator proceeds:

- a. (if not already done automatically by the IT platform) to the registration of the report on the register reserved for reports, assigning a unique progressive code, recording the date and time of receipt;
- b. once the report is displayed, to the notification of take-over to the reporter.

### B) Preliminary assessment phase

The reporting manager carries out a preliminary assessment of the report received, in order to check whether the report is among those that can be handled, in accordance with the procedure.



In the event that an 'unmanageable' report is received by the manager, feedback must be given to the reporter.

C) Preliminary investigation phase

In the event that the manager receives a 'manageable' report, the internal investigation of the reported facts or conduct must be initiated.

During the preliminary investigation phase, the reporting manager may avail himself of the support and cooperation of the competent corporate structures and, if necessary, of specific external expertise. The corporate structures involved in the verification activity guarantee the utmost timely cooperation and are bound by the same obligations of confidentiality and impartiality to which the reporting manager is bound. Employees carrying out support functions in the context of the management of disciplinary proceedings, as well as employees or persons who are or could be involved, albeit indirectly, in the violation that is the subject of the report, may not be part of the working group.

The reporting manager and each member of the team are under an obligation of absolute confidentiality as to the identity of the whistleblower.

The reporting manager and the members of the working group must abstain in the event of a conflict of interest, even if only apparent or potential, and are simultaneously required to report such a conflict to the Administrative Body.

The methodology to be used for the verification activities is assessed on a case-by-case basis, choosing the technique deemed most effective in relation to the nature of the event and the existing circumstances (interviews, document analysis, on-site inspections, technical consultations, research on public databases, checks on company equipment, etc.).

The reporting manager shall keep a record of the verification activities conducted. This documentation will be kept by the operator in a safe place.

During the investigation phase, the reporting manager maintains contact with the whistleblower and requests additions from the latter, if necessary.

The whistleblower may, at any time, request information from the reporting manager on the progress of the proceedings by sending a request to that effect.

The reporting manager, unless there are serious impediments (e.g. ongoing criminal investigations and corresponding secrecy obligations), responds to the request for information within 5 (five) working days from the date of receipt of the request.

Within 3 (three) months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within 3 (three) months from the expiry of the 7 (seven) day period from the submission of the report, the reporting manager shall provide feedback to the reporter.

The maximum time limit for concluding the proceedings is set at 160 (one hundred and sixty) days from the date of

receipt of the report (or, if no notice was sent to the whistleblower, 160 (one hundred and sixty) days from the expiry of the 7-day period from the date the report was made).

D) Notification phase of the outcome of the investigation

If the outcome of the investigation is unfounded, the report is closed. Upon conclusion of the investigation, the reporting manager informs the whistleblower of the outcome.

In relation to founded reports, the reporting manager makes any recommendations deemed appropriate, including the adoption of disciplinary measures or the proposal of a report to the Judicial Authority, the identification of any protective measures deemed necessary and the proposal of actions to close any organisational or control *gaps*.

The results of its checks, all observations, evaluations and decisions of the reporting manager, any recommendations and proposals for disciplinary measures shall in all cases be formalised in writing in an appropriate report communicated:

- a. to the head of the organisational unit of the reported person that made the ascertained infringement for the relevant measures;
- b. the Board of Directors for any further action that may be necessary to protect the Company (e.g. reporting to the competent Judicial Authority, adoption of new company procedures or amendment/integration of existing ones, organisational changes, etc.);
- c. to the Board of Statutory Auditors, in the event of competence.

The competent corporate functions implement these recommendations and corrective actions, the monitoring of which is carried out by the reporting manager.

Notification of the outcome of the investigation must normally take place by the end of the procedure.

### 13. CONFIDENTIALITY OBLIGATION

Report may not be used beyond what is necessary to adequately follow them up.

The identity of the reporter and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the whistleblower, to persons other than those responsible for receiving or following 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.

In criminal proceedings, the identity of the reporter is covered by secrecy in the manner and to the extent provided for in Article 329 of the Italian Code of Criminal Procedure.

In proceedings before the Court of Auditors ("Corte dei Conti"), 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 charge is based, in whole or in part, on the report and knowledge of the identity of the reporter is indispensable for the accused's defence, the report will be usable for the purposes of disciplinary proceedings only if the whistleblower has expressly consented to the disclosure of his identity.

The whistleblower shall be notified in writing of the reasons for the disclosure of confidential data, in the hypothesis referred to in the preceding paragraph, as well as in internal and external reporting procedures when the disclosure of the whistleblower's identity is also indispensable for the defence of the person concerned.

The report is exempt from access provided for in Articles 22 et seq. of Law No 241 of 7 August 1990 and Articles 5 et seq. of Legislative Decree No 33 of 14 March 2013.

#### **14. PROCESSING OF PERSONAL DATA**

All processing of personal data is carried out in accordance with Regulation (EU) 2016/679, Legislative Decree No 196 of 30 June 2003 and Legislative Decree No 51 of 18 May 2018.

Personal data that are clearly not useful for processing a specific report are not collected or, if accidentally collected, are deleted immediately.

The rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of Article 2-undecies of Legislative Decree No. 196 of 30 June 2003.

The processing of personal data relating to the receipt and handling of reports shall be carried out in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679 or Articles 3 and 16 of Legislative Decree No. 51 of 18 May 2018, providing appropriate information to the reporter and the persons involved pursuant to Articles 13 and 14 of the same Regulation or Article 11 of the aforementioned Legislative Decree, as well as taking appropriate measures to protect the rights and freedoms of the persons concerned.

#### **15. THE RETENTION OF DOCUMENTS RELATED TO THE REPORTS**

The report and the related documentation shall be retained for as long as necessary for the processing of the report and in any event no longer than 5 (five) years from the date of the communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in Article 12 and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of Legislative Decree No. 51 of 18 May 2018.

If a recorded telephone line or other recorded voice messaging system is used for the report, subject to the consent of the whistleblower, the report shall be documented either by recording it on a device suitable for storage and listening or by means of a verbatim transcript. In the case of a transcript, the reporter may verify, rectify or confirm the content of the transcript by signing it.

If an unregistered telephone line or other unregistered voice messaging system is used for reporting, the report shall be documented in writing by means of a detailed transcript of the conversation. The whistleblower may verify, correct and confirm the content of the transcript by signing it.

When, at the request of the person making the report, the report is made orally during a meeting with the reporting manager, it shall, subject to the consent of the whistleblower, be documented either by recording it on a device suitable for storing and listening to it or by taking minute. In the case of minute, the reporting person may verify, rectify and confirm the minute of the meeting by signing it.

## 16. THE WHISTLEBLOWER'S PROTECTION MEASURES

### I) Condition for Protection

The protective measures provided for by law apply only where, at the time of the report, the whistleblower had reasonable grounds to believe that the information on the reported violations was true and fell within the objective scope of paragraph 6 of this Procedure.

### II) Confidentiality of the whistleblower

The identity of the whistleblower and of other persons, in different capacities, connected to the report is protected at all stages of the procedure. Therefore, this information may not be disclosed to persons not directly involved in the assessment or investigation process.

The obligation to maintain strict confidentiality on the identity of the whistleblower and on the subject of the report applies to all persons who, for whatever reason, become aware of the report or are involved in the process of investigating it.

This protection also applies to the top management of the Company, which may not order investigations or request information in order to trace the identity of the whistleblower. Therefore, in the case of transmission of the report to other directorates, bodies or third parties for the purpose of carrying out investigative activities, the reporting manager shall forward only the content of the report, excluding all references from which it is possible to trace, even indirectly, the identity of the whistleblower.

The confidentiality of the whistleblower may not be respected when:

- there is the express consent of the whistleblower to the disclosure of his or her identity;
- the whistleblower may be held criminally liable, even by a judgment of first instance, for offences of slander or defamation or, in any case, for offences committed in connection with the report to the judicial authorities, or civil liability for the same offence, in cases of wilful misconduct or gross negligence; in such case, the Company reserves the right to carry out the necessary investigations against the whistleblower and to adopt the measures deemed appropriate.

Violation of confidentiality of the whistleblower's identity, except in cases where disclosure of his or her identity is

permissible as outlined above, is a source of disciplinary liability, for failure to comply with service provisions.

(III) The prohibition of retaliation

The whistleblower and the other persons referred to in IV) of this paragraph may not suffer any retaliation.

In the context of judicial or administrative proceedings or, in any case, out-of-court disputes concerning the ascertainment of the conduct, acts or omissions prohibited against the whistleblower, it shall be presumed that such conduct or acts were put in place as a result of the whistleblowing or disclosure or complaint. The burden of proving that such conduct or acts are motivated by reasons unrelated to the reporting or disclosure or complaint shall be on the person who has put them in place.

In the event of a claim for damages lodged with the Judicial Authority by the whistleblower, if the whistleblower proves that he or she has made a public report or disclosure under the Decree and has suffered damage, it shall be presumed, unless proved otherwise, that the damage is the consequence of such report or disclosure.

The following are examples of cases that constitute retaliation:

- a) dismissal, suspension or equivalent measures;
- b) relegation in grade or non-promotion;
- c) change of duties, change of workplace, reduction of salary, change of working hours;
- d) suspension of training or any restriction of access to it;
- e) negative merit notes or negative references;
- f) the adoption of disciplinary measures or other sanctions, including fines;
- g) coercion, intimidation, harassment or ostracism;
- h) discrimination or otherwise unfavourable treatment;
- i) the failure to convert a fixed-term employment contract into an employment permanent contract, where the employee had a legitimate expectation of such conversion;
- j) non-renewal or early termination of a fixed-term employment contract;
- k) 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;
- l) 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;
- m) early termination or cancellation of the contract for the supply of goods or services;
- n) cancellation of a licence or permit;
- o) the request to undergo psychiatric or medical examinations.

A whistleblower who believes that he or she has suffered discrimination as a result of having made a report must

give detailed notice of the discrimination to the reporting manager, who will assess whether there are grounds for informing the Board of Directors of what has happened so that it can take all necessary and appropriate steps.

The adoption of discriminatory measures against whistleblowers may be reported to the ANAC.

#### IV) Limitations on Liability

It is not punishable who, through his or her reporting:

- discloses or disseminates information on violations covered by the obligation of secrecy, other than professional, forensic or medical secrecy, or relating to the protection of copyright or the protection of personal data;
- discloses or disseminates information that offends the reputation of the reported person when:
  - a. at the time of disclosure or dissemination there were reasonable grounds to believe that the disclosure or dissemination of the information was necessary to disclose the violation;
  - b. the report was made under the conditions set out in the Decree.

In the event of a libellous or defamatory report under the Criminal Code and Article 2043 of the Civil Code, the criminal, civil and disciplinary liability of the whistleblower remains unaffected.

In particular, protections in favour of the whistleblower are not guaranteed in cases where the whistleblower's criminal liability for offences of slander or defamation or in any case for offences committed in connection with the report is established, even by a judgment of first instance, or in the event of civil liability, for the same reason, in cases of wilful misconduct or gross negligence.

Making malicious or grossly negligent reports that turn out to be unfounded is also a source of disciplinary liability. Any form of abuse of this procedure, such as reports that are manifestly opportunistic and/or made with the sole aim of harming the whistleblower or other persons, and any other hypothesis of improper use or intentional exploitation of the institution covered by this procedure, shall also give rise to liability in disciplinary and other competent court.

#### V) Support measures

It is possible for the whistleblower to obtain from ANAC a list of third-sector entities dedicated to providing him/her with support, advice and information, entirely free of charge.

#### VI) Beneficiaries of the protections

The aforementioned protection measures are also recognised in respect of the following persons, in order to prevent 'cross-retaliatory' conduct:

- (i) facilitators, i.e. those who assist the whistleblowe in the reporting process and whose assistance must be kept confidential;
- (ii) persons in the same employment context of the whistleblower, or the person who has filed a

- complaint with the judicial or accounting authorities or the person who has made a public disclosure and who are linked to them by a stable emotional or family relationship up to the fourth degree;
- (iii) co-workers of the whistleblower or of the person who has filed a complaint with the judicial or accounting authorities or made a public disclosure, who work in the same work environment as the whistleblower and who have a habitual and current relationship with that person;
- (iv) entities owned by the whistleblower or the person who filed a complaint with the judicial or accounting authorities or made a public disclosure or for which the same persons work, as well as entities operating in the same work environment as the aforementioned persons.

## 17. THE PROTECTION OF THE REPORTED PERSON

The Company requires everyone to cooperate in maintaining a company climate of mutual respect and prohibits attitudes that may harm the dignity, honour and reputation of each individual.

The whistleblower may not be subject to disciplinary sanctions in the absence of objective evidence of the reported violation, i.e. without investigating the reported facts and contesting the relevant charges in accordance with the procedures laid down by law and/or by contract.

In handling and managing reports, the necessary precautions must be taken to protect the confidentiality of the reported person. This is in order to avoid prejudicial consequences, even of a reputational nature, within the working context in which the reported person is placed.

The data on reported persons are in any case protected by the rules on personal data.

If the charge is based, in whole or in part, on the report and knowledge of the identity of the reporter is indispensable for the accused's defence, the report will be usable for the purposes of disciplinary proceedings only if the reporter expressly consents to the disclosure of his identity.

The whistleblower may be heard, or, upon request, shall be heard, also by means of a procedure through the acquisition of written observations and documents.

The protection of whistleblowers applies without prejudice to legal provisions imposing an obligation to disclose the name of the whistleblower (e.g. requests by judicial or accounting authorities).

## 18. EXTERNAL REPORTING

The whistleblower may only make an external report if, at the time of its submission, one of the following conditions is met:

- a) the internal reporting channel is not active or, even if activated, does not comply with the provisions of the Decree;
- b) the whistleblower has already made an internal report and it has not been followed up;

- c) the whistleblower has reasonable grounds to believe that, if he or she were to make an internal report, it would not be effectively followed up or that the report might give rise to the risk of retaliation;
- d) the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

In compliance with Article 7 of the Decree, the National Anti-Corruption Authority (ANAC) has activated a special external reporting channel.

Relevant information and instructions on external reporting managed by ANAC can be found on ANAC's website at:

<https://www.anticorruzione.it/-/whistleblowing>.

An external report submitted to a person other than ANAC must be transmitted to the latter, within 7 (seven) days of its receipt, with simultaneous notification of the transmission to the reporter.

## 19. PUBLIC DISCLOSURE

The whistleblower may only make a public disclosure if one of the following conditions is met at the time of submission:

- a) the whistleblower has previously made an internal and external report or has directly made an external report in the manner provided for by the Decree no response has been received within the time limits provided for by the Decree regarding the measures envisaged or adopted to follow up the reports;
- b) the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest;
- c) the whistleblower has reasonable grounds to believe that the external report may involve a 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 colluding with or involved in the perpetrator of the violation.

## 20. SANCTIONS

The following persons are liable to disciplinary action:

- whistleblowers who maliciously or grossly negligently make reports that turn out to be unfounded or 'in bad faith';
- the corporate entity that took discriminatory or retaliatory measures against the whistleblower;
- those who obstruct or attempt to obstruct reports;
- persons who engage in any form of abuse of this policy, such as reports that are manifestly opportunistic and/or made for the sole purpose of harming the whistleblower or other persons, as well as persons who engage in any other form of misuse or intentional exploitation of the institution covered by this



procedure.

- the internal reporting manager in the event of failure to carry out verification and analysis activities;
- those who do not guarantee the general principles of protection with particular reference to respect for the confidentiality of the whistleblower's identity;
- the reported person who, following the results of the checks carried out by the Company, was found to have carried out illegal or irregular acts, or activities not in compliance with the Code of Ethics, the organisational model pursuant to Legislative Decree No. 231/01 or the system of company procedures, also in accordance with the provisions of the disciplinary system of the collective labour agreement.

## 21. PUBLICITY OF THE PROCEDURE

The procedure is posted on the company notice boards and published on the company website and in a special section of the company intranet.

## 22. AWARENESS-RAISING INITIATIVES

Azimut Benetti undertakes initiatives to communicate and raise awareness of the procedure by means of training plans for all personnel on the purpose of the institution and its use, on the relative rights and obligations, on the consequences of abuses in its use, and on the results that the implementation of the rule has produced.

## 23. MODIFICATION OF MODEL 231 FOLLOWING REPORTS

If, as a result of the reports, objective elements emerge capable of revealing any critical aspects concerning the suitability and effectiveness of the Organisational Model pursuant to Legislative Decree 231/01, the Supervisory Board will propose the introduction of suitable amendments to the model itself.

## 24. PERIODIC REVIEW OF THIS PROCEDURE

This procedure may be subject to periodic revision approved by the administrative body and published on the company's website and in a special section of the company intranet.