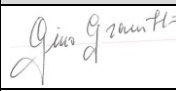
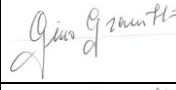
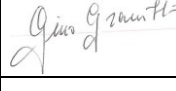


Registration of Reviews					
Rev.	Date	Description of the review	Prepared by	Checked by RSI	Approved by PRE
00	04/01/22	First issue following adaptation to Italian Model 231 and SA 8000	Federico Variati	Federico Variati	
01	15/02/22	Introduction of the certification body email	Federico Variati	Federico Variati	
02	24/11/22	Introduction ISO 37001 concepts and Whistleblowing	Federico Variati	Federico Variati	

Distribution list			
Acronym	Function	Acronym	Function
PRE	Chairman of the Board of Directors	CdA	Members of the Board of Directors
AMM	Administration Manager	ACQ	Procurement & Tender Manager
COG	Chief Financial Officer	COM	Chief Marketing Officer
RPV	Solar Division Manager	TEC	Chief Technology Officer
ROA	Water Operations Manager (Lombardia)	ROA	Water Operations Manager (Acerra)
RDW	Water Division Manager	ROW	Water Operations Manager (Colleferro)
RDM	Automation Division Manager	RSI	Quality, Health, Safety, and Environment Manager
RSP	Occupational Health and Safety Manager	RU	HR Manager
LEG	Legal & Compliance	RIN	IT Manager
RRS	Research and Development Manager	SPT	Social Performance Team
OdV	<i>Organismo di Vigilanza</i>	RPC	Anti-bribery Compliance Function
RLS	Workers' Safety Representative		

## Indice

1	Purpose and Scope .....	3
1.1	Foreword .....	3
1.2	Scope .....	3
2	Terms and Definitions .....	3
3	Reference Documents.....	5
4	Normative references .....	5
5	Subject of the report .....	5
6	Content of the report .....	6
7	Addressees of the procedure (whistleblowers) .....	6
8	Addressee of the report.....	7
9	Method of transmission of the report.....	7
10	The Whistleblowing Portal.....	8
11	Report Management.....	8
12	Protection and responsibility of the whistleblower .....	9
13	Protection of the reported person.....	10
14	Record keeping and privacy protection .....	10
15	Sanctions.....	11
16	Policy Update .....	11
17	Awareness.....	11
18	Attachments .....	11

## 1 Purpose and Scope

### 1.1 Foreword

On 29 December 2017, Italian Law No. 179 'Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship' came into force (published in the Official Gazette, General Series No. 291 of 14 December 2017).

The structure of the provision distinguishes the public sector (Art. 1) from the private sector (Art. 2), and the provision on the obligation of official, business, professional, scientific and industrial secrecy (Art. 3) has been supplemented.

As far as the private sector is concerned, Article 2 of Italian Law No. 179/17 intervenes on Italian Decree 231 and inserts a new provision in Article 6 ('Subjects in apical position and organisational models of the organisation) that frames within the organisational model of Italian Legislative Decree 231/01 the measures related to the presentation and management of reports.

The law aims to incentivise the cooperation of workers in order to encourage the emergence of corruptive phenomena within public and private entities, also by providing for systems that allow workers to safely report any wrongdoing they become aware of.

In fact, the law regulates:

- the prohibition of direct or indirect retaliatory or discriminatory acts against the whistleblower for reasons directly or indirectly linked to the report;
- the introduction of sanctions against those who breach the measures for the protection of the whistleblower, as well as against those who maliciously or grossly negligently make reports that turn out to be unfounded;
- the possibility for the whistleblower or the trade union organisation to report to the National Labour Inspectorate the adoption of discriminatory measures against whistleblowers;
- the nullity of retaliatory or discriminatory dismissals, as well as of job changes pursuant to Article 2103 of the Italian Civil Code, and any other retaliatory or discriminatory measures taken against the whistleblower;
- the onus on the employer, in the event of disputes relating to the imposition of disciplinary sanctions, or to demotions, dismissals, transfers, or subjecting the whistleblower to any other organisational measure having direct or indirect negative effects on working conditions, following the submission of the report, to prove that such measures are based on reasons extraneous to the report.

**Tea Tek** (hereinafter referred to as the "Company"), in the spirit of giving concrete application to Article 6 paragraph 2-bis lett. a) and b) of Italian Legislative Decree 231/2001, as introduced by Italian Law 179/2017, has made available to whistleblowers, in order to make reports, in addition to the traditional channel consisting of registered mail, a Whistleblowing Portal - suitable for guaranteeing, by means of computerised methods, the confidentiality of the identity of the whistleblower in the activities of managing reports.

### 1.2 Scope

The purpose of this procedure is to regulate the process of receiving, analysing and managing Reports submitted by staff and third parties in order to denounce unlawful phenomena and suspicious conduct, irregularities in company management, acts or facts that may constitute a breach of the rules, internal and external, governing the Company's activities, of the principles and rules of conduct contained in the Code of Ethics, and of the provisions contained in the Italian Organisational Model 231 and in the Management System, adapted to the SA 8000 and ISO 37001 standards, adopted by the Company.

## 2 Terms and Definitions

Terms, acronyms and definitions can be found in the SGI Manual, the reference documents and Italian Legislative Decree 81/2008. Below are those of interest for this procedure:

**CdA (Board of Directors):** Collegiate body entrusted with the management of the joint-stock company;

**Chairman of the Board of Directors:** Member of the CdA who chairs the board of directors. Holds the legal representation of the company and is obliged to act in accordance with the resolutions of the Board of Directors. Defines company policy and strategies. Also referred to as Employer;

**SPT (Social Performance Team):** Term used to refer to a "mixed" working group consisting of Workers' Representatives for SA 8000 and management representatives. This team has a crucial role in the implementation of SA8000, as it is required to conduct periodic written risk assessments to identify and prioritise areas of actual or potential non-compliance with the standard.;

**Audit:** Activity to measure the conformity of certain systems, processes, products to certain required characteristics and to verify their application;

**Employer:** Person in charge of the employment relationship within which the worker works or, in any case, has responsibility for the organisation itself or the production unit as he/she exercises decision-making and spending powers;

**Non Conformity:** is defined as "non-compliance with specified requirements", or even "anomalies", "inconveniences", "deficiencies", "incorrect behaviour" found in the performance of company activities, to the extent that such situations are in conflict with specifications, provisions, directives, standards, procedures, technical constraints, etc. that regulate the activities themselves or in any case are in conflict with the functionality of the service provided;

**Organismo di Vigilanza (OdV):** indicates a body to oversee the criminal liability of entities, for offences committed in their interest or to their advantage;

**Workers' Safety Representative:** "Person elected or designated to represent workers with regard to aspects of health and safety at work". This is the figure who represents other workers in the field of safety and prevention in the workplace. Not to be confused with or considered as a representative, he is in fact the intermediary between the Employer and the workers themselves. The Workers' Safety Representative collects all requests, in the field of safety and health, from all other workers in order to bring them to the Employer, with the aim of improving the company;

**Occupational Health and Safety Manager (RSPP):** This is the figure in possession of the requirements and capacities set out in Art. 32 D. Italian Legislative Decree 81/2008. To perform the specific functions, a certificate of attendance, with verification of learning, at specific training courses appropriate to the nature of the risks present in the workplace and related to the work activities is required. The RSPP essentially performs technical and organisational support functions and tasks for the employer, managers, and supervisors; he also has relational tasks with workers and their representatives (e.g. information to workers), also on specific problems concerning the company;

**Quality, Health, Safety, and Environment Manager:** This function is responsible for implementing the Integrated Management System on the basis of the objectives defined by the Management and for ensuring that the System complies with the reference standards (e.g. ISO 9001, ISO14001, etc.). With reference to a specific standard, e.g. ISO 9001, he assumes the role of Quality Assurance;

**Anti-bribery Compliance Function:** The person(s) with responsibility and authority for the operation of the management system for the prevention of corruption;

PRE	Chairman of the Board of Directors;
CEO	Chief Executive Officer;
MI	Integrated Management System Manual;
OdV	<i>Organismo di Vigilanza</i> ;
RPC	Anti-bribery Compliance Function;

RSI Quality, Health, Safety, and Environment Manager;  
SGI Integrated Management System;  
SPT Social Performance Team.

### 3 Reference Documents

- ❖ Integrated Management System Manual (MI);
- ❖ Social Responsibility System Manual (MRS);
- ❖ Italian organisational model 231;
- ❖ Code of Ethics;
- ❖ Social Responsibility Policy AL10MI01-POL;
- ❖ PR01-DOC "Documentation and communication management";

### 4 Normative references

- ❖ Italian Legislative Decree 231/01 'Regulations on the administrative liability of legal entities, companies and associations, including those without legal personality, pursuant to Article 11 of Italian Law No. 300 of 29 September 2000' of 08/06/2011 and subsequent updates;
- ❖ Italian Legislative Decree No. 196 of 30 June 2003 - Personal Data Protection Code - and subsequent amendments and/or variations;
- ❖ EU Regulation 2016/679 of the Parliament and of the Council of 27 April 2016 on the Protection of Individuals with regard to the Processing of Personal Data;
- ❖ Italian Law No. 179 of 30 November 2017 'Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship';
- ❖ SA 8000:2014 (Social Accountability International) international standard on corporate social responsibility;
- ❖ UNI ISO 37001:2016 "Anti-bribery management systems — Requirements with guidance for use".

### 5 Subject of the report

The obligation to report applies whenever the addressee of the Model has a reasonable and legitimate suspicion or awareness - both based on precise and concordant factual elements - of criminal conduct or of conduct aimed at circumventing the prescriptions of the Model carried out by other addressees (whether or not of senior management level).

In particular, the relevant report concerns two types of conduct:

- unlawful conduct relevant under Italian Legislative Decree No. 231/01, i.e. conduct that is criminally relevant insofar as it may constitute "predicate" offences referred to in Italian Legislative Decree No. 231/01, even in the form of a mere attempt, of which the Addressees have become aware on the basis of serious, precise and concordant factual elements;
- violations of the Code of Ethics, of the 231 Organisational Model and of the internal procedures of the SGI based on precise and concordant factual elements, of which the Addressees have become aware by reason of the functions performed. In such a case, the report concerns conduct which, even if it has no direct criminal relevance, in any case contravenes the crime prevention system put in place by the Company, since it violates the control principles (general or specific), the safeguards or company procedures referred to in the 231 Organisational Model.

Non-exhaustive examples of possible alerts relevant for the above purposes include:

- conflict of interest situations not known to the company;
- attempts/acts of corruption by directors or employees towards third parties (public officials or even private individuals);
- fraud committed in the interest of the company;
- intentional communication of false information to public authorities.
- corporate or business transactions for which it is suspected that a sanction risk may arise for the Company pursuant to Italian Legislative Decree 231/01;

- situations of non-compliance or alleged non-compliance with one or more requirements of SA 8000, consistent with the social responsibility policy adopted by the company;
- situations of corruption or alleged non-compliance with one or more requirements of ISO 37001.

The following will not be worthy of mention:

- Mere rumours or 'hearsay';
- The whistleblower's personal grievances or claims/ claims.

Reports must be made in good faith, in a spirit of responsibility, be of interest to the common good, fall within the types of non-compliance for which the system has been implemented.

## 6 Content of the report

Reports should not contain surplus data, but only the data necessary to prove the justification of the complaint. As a general rule, therefore, no special data\* or personal data revealing health or judicial status should be included. Should the reports contain the aforementioned categories of personal data referring to the reporter or to third parties, and should these data not be necessary for the pursuit of the aforementioned purposes, the company shall destroy them or, if this is not possible, obscure them, except in cases authorised by law or by an order of the Data Protection Authority.

If the report does not fall within the competence of the OdV, the SPT or the RPC according to the definition of the objective scope just described, the OdV will urge the reporting person to forward it to the competent corporate area/body and/or to the competent Authorities. Such reports are, in any case, considered 'protected'. This means that the reporting body does not disclose the identity or personal data of anyone who has forwarded such a report without having first obtained their explicit consent - unless disclosure is required by law, by investigations or subsequent legal proceedings.

In all the above-mentioned cases of communication, the Controller guarantees that appropriate measures will always be taken to avoid unnecessary circulation of information, in order to ensure appropriate confidentiality in view of the particular purposes of the processing in question.

*\*information revealing racial or ethnic origin, sexual orientation, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade-unionist character.*

## 7 Addressees of the procedure (whistleblowers)

In particular, the Addressees of this procedure are:

- top management and members of corporate bodies;
- employees, customers, suppliers, consultants, collaborators and, more generally, anyone in a relationship of interest with the company.

Recipients who are aware of facts that are potentially the subject of a report are required to make the reports, providing all the elements that are useful for carrying out the checks and investigations necessary to assess their justification, and indicating at least the following elements:

- Unless the report is anonymous, the identity of the person making the report, with an indication of the position or function held within the company;
- description of the reported facts with an indication of the known circumstances (manner, time and place) relating to the reported facts;
- any information or evidence that may provide useful feedback as to the existence of the reported facts, in particular also the indication of any other persons who may report on the reported facts;
- the absence of any private interest connected to the report and its good faith;
- identifying elements of the Reported;
- any other information deemed relevant to the report.

## 8 Addressee of the report

In the event of non-compliance, or alleged non-compliance, with the Model 231 adopted by the company, the OdV pursuant to Italian Legislative Decree 231/2001 is the recipient of reports of offences.

In the case of non-compliance, or alleged non-compliance, with SA 8000 (social accountability) requirements, the SPT or the RSI are the recipients of reports. Any other reporting channels (external to the company - SAI channel and Certification Body) are listed in the Social Responsibility Policy AL10MI01-POL.

In the case of non-compliance, or alleged non-compliance, with ISO 37001 (anti-bribery) requirements, the RPC is the recipient of reports.

The addressees ensure the proper conduct of the process of reporting violations and report, directly and without delay, to the Administrative Body the information reported, if the violation has been ascertained.

The OdV, as Recipient of the Report:

- is autonomous and independent of the operational functions, not depending hierarchically on any of them;
- ensures a fair and impartial judgement on the report received;
- respects the confidentiality obligations of the whistleblower and the reported person.

The SPT, as Recipient of the Report:

- analyses incoming reports and takes action to prepare treatment, collaborating in the identification of corrective actions;
- ensures a fair and impartial judgement on the report received;
- respects the confidentiality obligations of the whistleblower and the reported person.

The RPC, as Recipient of the Report:

- analyses the reports received and takes action to prepare appropriate investigations in relation to the reported corruption events;
- ensures a fair and impartial judgement on the report received;
- respects the confidentiality obligations of the whistleblower and the reported person.

## 9 Method of transmission of the report

A Whistleblower, if he/she has a reasonable suspicion that one of the above-mentioned violations according to Model 231 has occurred or may occur, has the possibility of making a Report to the OdV using the following channels:

- Through e-mail :[odvteatek@gmail.com](mailto:odvteatek@gmail.com)
- Through registered mail with return receipt to the address of the company T.E.A. Tek S.p.A., Via Maddaloni snc Consorzio Area 80011 Acerra (NA), addressed to the OdV;
- Through the Whistleblowing Portal, as specified in the next paragraph.

A Whistleblower, if he/she has a reasonable suspicion that a breach has occurred or may occur that goes against the SA 8000 principles adopted by the company, has the opportunity to make a Report using the following channels:

- Through e-mail [spt.teatek@gmail.com](mailto:spt.teatek@gmail.com);
- Through e-mail [crs@it.bureauveritas.com](mailto:crs@it.bureauveritas.com);
- Through the SAI portal <https://sa-intl.org/services/assurance/sa8000-complaints-and-feedback/>;
- Through the Whistleblowing Portal, as specified in the next paragraph.

A Whistleblower, if he/she has a reasonable suspicion that a breach has occurred or may occur that goes against the ISO 37001 principles adopted by the company, has the opportunity to make a Report using the following channels:

- Through e-mail [anticorruzione.teatek@gmail.com](mailto:anticorruzione.teatek@gmail.com);
- Through registered mail with return receipt to the address of the company T.E.A. Tek S.p.A., Via Maddaloni snc Consorzio Area 80011 Acerra (NA), addressed to the RPC;
- Through the Whistleblowing Portal, as specified in the next paragraph.

## 10 The Whistleblowing Portal

The Whistleblowing Portal can be reached for Whistleblowers at the following dedicated web address:

<https://teatekspa.whistlelink.com/>

The platform allows anyone (employees and collaborators, suppliers and any other person who has had or intends to have business relations with the Company) - through a guided on-line path - to make reports, guaranteeing the anonymity of the reporter; the system, in fact, allows reports to be sent without the obligation to register or state personal details. If the whistleblower chooses to indicate his or her personal details, confidentiality is guaranteed.

The platform enables a confidential dialogue with the reporter, with no possibility for the receiver or others to trace the origin of the report.

Access to the Whistleblowing Portal is, in fact, subject to the "no-log" policy in order to prevent the identification of whistleblowers who wish to remain anonymous: this means that the company's IT systems are not able to identify the portal access point (IP address) even if access is made from a computer connected to the company network.

Reports transmitted via the Whistleblowing Portal are received exclusively by members of the OdV. The association of the identity of the whistleblower with the report can, in fact, only be carried out by the body in charge of handling the reports (OdV - *Organismo di Vigilanza*).

The data contained in the reports will be processed using organisational and processing methods that guarantee the security, integrity and confidentiality of the data, in compliance with the organisational, physical and logical measures provided for by the provisions in force.

In particular, the transmission of data provided by the reporter using the platform is managed using the HTTPS protocol. Encryption techniques are also applied, thus guaranteeing the confidentiality of the information transmitted.

Anonymous reports, i.e. reports made without identification of the whistleblower, will be taken into account if they are adequately substantiated and made in full detail, i.e. if they are able to bring to light facts and situations relating to specific contexts.

After accessing the Portal, the whistleblower will be guided in filling in a questionnaire consisting of open questions that will allow him/her to provide the elements characterising the report (facts, temporal context, economic dimensions, etc.).

When filling in this form, the Portal will ask the reporter whether or not he intends to reveal his identity. In any case, the reporting person may also provide his or her identity at a later stage, through the messaging system provided by the Portal.

When sending the report, the Portal will issue the whistleblower with a unique identification number. This number, known only to the whistleblower, cannot be recovered in any way in the event of loss. The code will be used by the reporter to access his or her report through the Portal in order to: monitor the progress of the report; enter further information to substantiate the report; provide personal details; answer any further questions.

## 11 Report Management

Reports received by members of the OdV, the SPT or the RPC are subject to the following investigation procedure.

Reports whose vagueness does not even make it possible to initiate a verification by directing it towards



concrete prospects will not be taken into account and will be immediately archived.

The reports and their supporting documents shall be subject to preliminary analysis by the OdV, the SPT or the RPC, in order to verify the presence of useful and sufficient data and information to assess the abstract justification of the report in order to initiate further investigations.

Once this analysis has been carried out, if the OdV, the SPT or the RPC verifies that the fact reported does not have an impact for the purposes of Italian Legislative Decree 231/01, SA 8000 or ISO 37001, but may nevertheless be relevant for the Company, it will invite the reporting party to forward it to the competent body/organisation.

In the event, on the other hand, that the OdV, the SPT or the RPC deems that there is a reasonable assumption of foundation/reliability, an in-depth investigation will be carried out on the facts that are the subject of the report, in order to ascertain whether they are well-founded. In carrying out the aforementioned analysis, the Addressee may avail himself/herself - for specific aspects dealt with in the reports and where deemed necessary - of the support of other corporate functions within the scope of their competence, and may request further information and/or documentation from the reporter through the portal.

If, at the end of the preliminary analysis phase, it emerges that there are no sufficiently circumstantiated elements or that the facts referred to are unfounded, the report will be filed with the relevant reasons. In such a case, the OdV, the SPT or the RPC will inform the reporting person of the conclusion and the results of the investigation carried out.

If, following the preliminary analysis, useful and sufficient elements emerge or can be deduced to assess the report as well-founded, the subsequent phase of specific investigations will be initiated.

The OdV / SPT / RPC will:

- initiate specific analyses using, if deemed appropriate, the competent structures of the Company;
- agree with the management in charge of the function concerned by the report, the possible action plan necessary for the removal of the control weaknesses detected;
- agree with the CEO and the Functions concerned on any initiatives to be taken to protect the interests of the Company;
- request, if possible, the initiation of disciplinary proceedings against the whistleblower, in the case of reports in which the whistleblower's bad faith and/or purely defamatory intent is established, possibly also confirmed by the groundlessness of the report itself;
- upon conclusion of the investigation carried out, submit the results to the CEO or the Board of Statutory Auditors, depending on the subject of the report, for appropriate action to be taken;
- terminate the investigation at any time if, in the course of the investigation, it is established that the alert is unfounded.

The activities described above are not necessarily carried out sequentially.

## **12 Protection and responsibility of the whistleblower**

The Company guarantees the confidentiality of the whistleblower's identity from the stage of receipt of the report, in compliance with the provisions of the law. To this end, the personal data identifying the reporter are not directly visible in the report and are stored so as to be visible only to the body in charge of handling the report. The company adopts all the guarantees provided for by law in order to protect the confidentiality of the whistleblower's identity, so that it is not disclosed to third parties without the latter's express consent, except in the case of whistleblowing in bad faith or defamatory reports.

No retaliation or discrimination, direct or indirect, may result against a person who has made a report in good faith, regardless of whether or not the report turns out to be well-founded.

Sanctions are provided for those who breach the whistleblower protection and confidentiality measures.

On the other hand, the protection of the whistleblower is not guaranteed in the case of reports made with

malicious intent or gross negligence or that turn out to be false, unfounded, defamatory or otherwise made with the sole purpose of harming the Company, the reported person or other persons concerned by the report.

In the event 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 and additional to the report, even if consequent to it; the identity of the whistleblower may only be disclosed if:

- the charge is based, in whole or in part, on the report itself and knowledge of the identity of the whistleblower is absolutely essential for the accused's defence;
- there is consent of the whistleblower.

Penalties are provided for the whistleblower, should he or she be traced in the event of reports made with malicious intent or gross negligence or which prove to be false, unfounded, defamatory or otherwise made with the sole purpose of harming the Company, the reported person or other persons concerned by the report.

The Company may also take the appropriate legal steps.

### **13 Protection of the reported person**

The Company guarantees adequate protection for persons directly or indirectly subject to the report.

The report is not sufficient to initiate any disciplinary proceedings against the reported person.

It will therefore not be possible to impose disciplinary sanctions on the reported person on the basis of what the whistleblower alleges, without objective evidence and without investigating the reported facts.

This could possibly be done on the basis of other evidence found and ascertained from the report itself.

If the OdV, the SPT or the RPC, following the concrete findings of the report, decides to proceed with the preliminary investigation, the reported person may be contacted and given the opportunity to provide any necessary clarification.

### **14 Record keeping and privacy protection**

The personal data provided by the whistleblower at the time of registration and the information contained in the reports and in any documents attached to them, as well as any data acquired during the investigation by the body in charge, are processed in accordance with the Personal Data Protection Policy adopted by the Company, in compliance with the principles of fairness, lawfulness, transparency and protection of the confidentiality and rights of all those concerned (whistleblower, reported and any third parties involved), and in compliance with the obligations imposed by the privacy legislation and Italian Law no. 179, concerning "Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship".

The OdV / the SPT / the RPC takes care of filing all the documentation supporting the report received. Personal data relating to reports are retained and kept for the period necessary to complete the verification of the facts set out in the report and for 5 years after the report is closed, except for any proceedings arising from the handling of the report (disciplinary, criminal, accounting) against the reported person or the whistleblower (bad faith, false or defamatory statements). In this case, they will be kept for the duration of the proceedings and until the expiry of the time limit for challenging the relevant measure.

The personal data contained in Reports may be communicated to the competent offices of the Company for the activation of judicial and/or disciplinary protection related to the report, or to the competent Authorities in the event of violations of applicable regulations.

All details concerning the processing of the personal data of the data subjects involved in the report are provided in the processing notice pursuant to Article 13 GDPR, administered when the report is submitted through the platform and attached hereto.

## 15 Sanctions

Violation of the principles laid down in this procedure shall be prosecuted, promptly and immediately.

Tea Tek reserves the right to take disciplinary action against the whistleblower in the event of abuse of the Whistleblowing tool, for example in the event of manifestly opportunistic reports and/or for the sole purpose of damaging the reported person or persons concerned by the report and any other hypothesis of improper use or intentional exploitation of the institute covered by this procedure.

Sanctions will be applied on the basis of the Workers' Statute (Italian Law No. 300/1970) and individual National Collective Bargaining Agreements.

## 16 Policy Update

This Procedure and the Whistleblowing Portal will be subject to periodic review to ensure constant alignment with the relevant legislation as well as in accordance with the operations and experience gained.

## 17 Awareness

The organisation undertakes initiatives to communicate and raise awareness of this procedure by means of dissemination on the company server and through training initiatives aimed at all staff in order to communicate the purpose of reporting, the institution of Whistleblowing and how to use it correctly; on the related rights and obligations; on the consequences of abuses in its use; on the results that the implementation of the rule has produced.

## 18 Attachments

- MO01PR21-SEG "SA8000 Reporting";
- Privacy Policy for whistleblowers