

Contact methods

Supervisory Body (SB)

- By registered letter a/r addressed to the attention of the SB, in Via Nazionale, 4/F - 24060 Casazza (BG); the report must be managed by using two closed envelopes, in order to separate the identifying data of the whistleblower from the alert;

1. the first with the identifying data of the whistleblower along with the photocopy of the identification document;

2. the second with the actual alert

The two envelopes must be placed inside a closed third envelope that bears the words "reserved for the sb".

The alert shall be recorded in confidence, including by an independent register, by the SB.

- Verbally, by declaration issued and reported on record by one of the parties entitled to receive.

WHISTLEBLOWING PRIVACY POLICY PURSUANT TO ART. 13 and 14 OF REGULATION (EU) 2016/679

a) What is the purpose of the policy?

In compliance with the provisions of the current legislation on the protection of personal data, i.e. EU Regulation 2016/679 (also known as "GDPR") and, as far as applicable, by complementary national legislation, we wish to inform you about the processing of personal data carried out by the Data Controller concerning the management, in all its phases, of the reports of persons who report violations of national or European Union regulatory provisions, of the reported and of any third parties involved (e.g. persons affected by the report, facilitators, etc.), as required by Legislative Decree no. 24 of 10 March 2023.

We assure you that the processing will be based on the principles of correctness, lawfulness and transparency, as well as the protection of your privacy and the protection of your rights **and with security measures that protect you against any possibility of retaliation against you.**

This information is provided for the personal data that you provide in the context of whistleblowing reports.

b) Who is the Data Controller? How to contact him?

The Data Controller is Mobility Technical Management Italia S.r.l. with registered office in **Borgo Di Terzo (BG) Via Roma 1, C.F./P.IVA 03355520168**, hereinafter referred to as the "Data Controller". For the processing of reports, the Data Controller can be contacted at the following address: **TEOREMA SERVIZI DI PELLEGRINELLI ANGELO with registered office in Via Nazionale, 4 Casazza (BG).**

c) What categories of personal data do we process?

In order to handle the report, we must process personal data and any information necessary for the proper conduct of the investigation and to follow up on the report.

The data will be provided directly by you or from the reports received.

d) For what purposes is the data processed? On what legal basis? And how long are they stored?

Below we indicate the purposes of the processing, the legal basis that legitimizes the processing and the retention period of your personal data:

<i>Purpose</i>	<i>Legal basis</i>	<i>Preservation</i>
1. Whistleblowing and management of reports: to manage reports of unlawful conduct, conduct, acts or omissions that harm the interest or integrity of the organization, using the whistleblowing channels made available by the Data Controller in accordance with current legislation.	Legal obligation pursuant to Legislative Decree 23/2023 ("whistleblowing" decree). The fulfilment of obligations or the exercise of rights of the Data Controller or the data subject in the field of labour law and social security and social protection, pursuant to art. 9(2)(b) GDPR, for the processing of special categories of data.	For the duration necessary for the management of the report, and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure

e) Is it mandatory to provide the data? What happens if it doesn't provide them?

The provision of your personal data for the purpose of **Whistleblowing and management of reports** is necessary to follow up on the whistleblowing procedure.

f) Who can know your data? To whom do we communicate them?

Personal data relating to processing for whistleblowing purposes may only be known by a very limited number of persons authorised to process them and who have received specific instructions to ensure their confidentiality. In addition, your data may be known

- by the public administration, where required by law;

➤ by third parties who carry out processing on behalf of the Data Controller, such as management services of the technological platform responsible for the management of the internal reporting channel. These subjects are authorized to process them as Data Processors in accordance with the provisions of Article 28 of the GDPR. Of course, your personal data will not be disseminated.

g) Is personal data transferred outside the European Union (EU)?

The data collected is not transferred to locations outside the European Union.

h) What are your rights as a data subject?

The GDPR grants you the following rights in relation to your personal data, which you may exercise within the limits and in accordance with the provisions of the law:

- Right of access to your personal data (art. 15);
- Right to rectification (art. 16);
- Right to erasure (right to be forgotten) (art. 17);
- Right to restriction of processing (Art. 18);
- Right to data portability (art. 20);
- Right to object (art. 21); You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data concerning you based on legitimate interest, including profiling on the basis of legitimate interest. The Data Controller refrains from processing unless it demonstrates the existence of compelling legitimate reasons to proceed with the processing that prevail over the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of a right in court;
- Right to object to a decision based solely on automated processing (Art. 22);
- The right to revoke, at any time, the consent given, without prejudice to the lawfulness of the processing based on the consent given before its withdrawal.

You may exercise these rights by sending a request through the channel made available by the Data Controller as indicated above.

In addition, you have the right to lodge a complaint with the Data Protection Authority (www.garanteprivacy.it) if you believe that the processing of your data is contrary to the regulations in force (Article 77) or to take legal action (Article 79).

In any case, these rights may not be exercised if the exercise of these rights could result in an actual and concrete prejudice to the confidentiality of the identity of the person reporting violations.

i) How is personal data protected?

Personal data will be processed both electronically and without the aid of electronic tools, using technical and organizational security measures appropriate to the nature of the data to ensure their integrity and confidentiality and protect them against the risks of unlawful intrusion, loss, alteration, or disclosure to third parties not authorized to process them.

j) Updates

The Data Controller reserves the right to modify and update this policy at any time. It is therefore necessary for you to regularly check the Notice in force.

Edition of **08.01.2024**

INDEX

CAP.1 PURPOSE..... 2

CAP.2 SCOPE OF APPLICATION 2

CAP.3 RESPONSIBILITIES..... 3

CAP.4 WHISTLEBLOWER PROTECTION MEASURES 3

4.1 Confidentiality obligations on the identity of the whistleblower..... 3

4.2 Disclosure of information covered by the duty of secrecy 3

4.3 Prohibition of retaliation or discrimination 4

4.4 Reporting methods and recipients 4

4.5 Content of reports..... 6

CAP.5 DISSEMINATION AND TRANSPOSITION 6

CAP.6 ARCHIVING AND RETENTION 6

CAP.7 LEGISLATIVE AND REGULATORY REFERENCES 7

CAP.8 ADMINISTRATIVE PENALTIES..... 9

CHAP.9 INDICATIONS AND INFORMATION FLOWS TO THE SBV 10

CHAP.10 RELATED DOCUMENTS AND FILES 10

REVISION	DATE	DRAFTED: RS	VERIFIED AND APPROVED: RG
00	01/03/2022		
01	13/09/2023		

HISTORY OF CHANGES MADE.

None: This is the first version of the document.

01: Change in Corporate Manager and Communication Channels

Zip code.1 PURPOSE

The final approval of **Whistleblowing** marked a significant turning point for a more pervasive diffusion of internal systems for reporting violations with regard to the private sector with significant amendments to Legislative Decree no. 231/01, regarding the administrative liability of legal persons, companies and associations and introduces specific provisions governing any violations of the 231 Organization and Management Models, effectively extending the subjective scope of internal breach reporting systems.

The purpose of this process is to protect employees who report crimes or irregularities of which they have become aware for work reasons and to inculcate a "social conscience" within the workplace, which encourages the individual to take action to report to the authority or even to his employer, any offenses of which he or she has become aware in the performance of his or her work duties.

The procedure also aims to remove possible factors that may discourage the use of reporting, such as doubts and uncertainties about:

- The procedure to follow
- Fears of retaliation or discrimination by top management, superiors, etc.
- The possible disclosure of office, professional, scientific or industrial secrets.

In this perspective, the purpose pursued by this procedure is to provide the whistleblower with clear operational indications on the subject, contents, recipients and methods of transmission of the reports, as well as the forms of protection offered in our legal system.

CHAP.2 SCOPE OF APPLICATION

This procedure applies:

- Persons who hold functions of representation, administration or management of the entity or of one of its organizational units with financial and functional autonomy as well as by persons who exercise, even de facto, the management and control of the same
- Persons under the direction or supervision of any of the above-mentioned persons.

The reporting, by the above-mentioned personnel, must in any case be based on good faith or reasonable belief, of detailed reports of unlawful conduct, relevant pursuant to this decree and based on precise and consistent factual elements, or of violations of the organizational model and of the entity, of which they have become aware due to the functions performed.

All reports received, in the form and manner described below, will be processed by the Supervisory Body (SB) in compliance with this Management System, the provisions of the law, the Company Code of Ethics, as well as the instructions provided in accordance with the provisions of the Whistleblowing Decree Legislative Decree 24/23.

Anonymous reports, i.e. reports without elements that allow their author to be identified, delivered in the manner provided for in this document, are included in the scope.

However, anonymous reports will only be processed if they refer to particularly serious episodes and in the presence of clear, detailed, precise and consistent elements.

The requirement of the truthfulness of the facts or situations reported remains unchanged, in order to protect the reported person.

CHAP.3 RESPONSIBILITIES

The management of reports, as written above, is delegated to the Supervisory Body. This can be used with other functions to:

- Log incoming communications and keep up to date All-24.2 "Whistleblowing - Register of reports"
- Guarantee the preservation and privacy of the original documentation relating to the reports in special paper/computer archives, with the highest standards of security/confidentiality
- Monitor communication channels (regular and registered mail)
- Monitor communication channels (dedicated e-mails and internet communication tools)
- Evaluate approval of requests for the adoption of organizational measures and/or the imposition of sanctions or disciplinary measures and/or the initiation of legal proceedings
- Update and make available the All-24.1 "Whistleblowing" reporting forms
- Once the existence of the elements has been assessed, report the hypothesis of discrimination to the employee's Head of Function.

CHAP.4 WHISTLEBLOWER PROTECTION MEASURES

4.1 Confidentiality obligations on the identity of the whistleblower

The organization shall ensure that the information collected, relating to the report, remains confidential, except in cases where:

- The whistleblower gives his/her consent to the disclosure (processing) of his/her personal data
- It is required by law (e.g. if it is necessary to involve the Authorities)
- Whether aimed at safeguarding people's health or safety
- It is indispensable to the defence, during the hearing of the accused, for the purpose of presenting defence briefs; indispensability must be justified and demonstrated
- Liability for slander or defamation is possible.

All those who receive or are involved in the handling of reports are required to protect the confidentiality of such information.

Unauthorized disclosure of the identity of the whistleblower or information from which the same can be inferred, is considered a violation of this Management System.

Violation of the duty of confidentiality is a source of disciplinary liability, without prejudice to other forms of liability provided for by law.

4.2 Disclosure of information covered by the duty of secrecy

For the reports made, in the forms and within the limits described below, the Organization recognizes the protection of personnel pursuant to Legislative Decree no. 231/2001 in the event of disclosure of information covered by the obligation of office, business, professional, scientific and industrial secrecy.

When information and documents that are communicated to the Supervisory Body responsible for receiving them are subject to business, professional or official secrecy, disclosure in a manner exceeding the purposes of eliminating the offence and, in particular, disclosure outside the communication channel specifically set up for this purpose constitutes a breach of the relevant duty of secrecy.

The discriminating factor does not apply in the event that the obligation of professional secrecy is imposed on the person who has become aware of the news, due to a relationship of professional advice or assistance to the Organization, or in the event that the secrecy is revealed outside the specific channels of communication.

4.3 Prohibition of retaliation or discrimination

"Retaliatory" and/or "discriminatory" means the measures and actions taken against the employee who has reported, in particular:

- Unjustified disciplinary actions (degradation, non-promotion, transfer, dismissal, etc.)
- Harassment in the workplace (mobbing, persecution, etc.)
- Any other form of retaliation that leads to intolerable working conditions (isolation, threats, etc.).

The Organization does not allow and does not tolerate any form of retaliation or discriminatory measures, affecting the working conditions of the employee who makes a report for reasons directly or indirectly related to the complaint. The whistleblower also has the right to request transfer to another office and, where reasonably possible, the Organisation must provide for the fulfilment of such requests.

The protection is limited to cases in which the whistleblower and the reported are both employees of the same Organization.

An employee who believes he or she has been discriminated against for having made a report, reports the facts to the Supervisory Body which, after assessing the existence of the elements, reports the hypothesis of discrimination:

- To the employee's Function Manager and to the Human Resources Manager, who promptly assess:
 1. The advisability/necessity of taking measures to restore the situation and/or remedy the negative effects of discrimination
 2. The existence of the grounds for initiating disciplinary proceedings against the employee who committed the discrimination.

Requests for the adoption of organizational measures and/or the imposition of sanctions or disciplinary measures and/or the initiation of legal proceedings are the responsibility of the Management for approval.

This procedure is without prejudice to the criminal and disciplinary liability of the whistleblower in the event of slanderous or defamatory reporting pursuant to the Criminal Code and Art. 2043 c.c.

Any form of abuse of this procedure, for the sole purpose of damaging the person reported or for opportunistic purposes, is also a source of liability, in disciplinary proceedings and in other competent bodies.

4.4 Reporting methods and recipients

The Organization makes available to all people who work, in any capacity:

- The Whistleblowing Form, ALL-24.1 "Whistleblowing"
- Instructions for reporting, ALL-24.3 "Whistleblowing – Instructions for reporting corrupt acts"
- The Privacy Policy [SGP].

The form, instructions and information are made available, updated and transmitted to all employees of the Organization.

The report must be addressed to:

- To the Supervisory Body as it is appointed by the Management to manage reports relating to the predicate offences of the MOG pursuant to Legislative Decree no. 231/2001 adopted by the organisation.

The report received by any other employee of the Organisation must be promptly forwarded to the Supervisory Body, which is entrusted with the confidential registration and keeping of the relevant ALL-24.2 "Whistleblowing - Register of reports".

The transmission of the report must take place in compliance with the criteria of maximum confidentiality and in a manner suitable to protect the whistleblower and the identity and integrity of the reported subjects, without prejudice to the effectiveness of the subsequent investigation activities.

The Organization, following the provisions of Article 2bis inserted by Law 179/2017, has set up several channels that allow the submission of detailed reports of corrupt conduct or violations, relevant pursuant to this Management System, based on precise and consistent factual elements, of which they have become aware due to the functions performed.

These channels guarantee the confidentiality of the identity of the whistleblower in the management and processing of the report, which is submitted in the following ways:

- By registered letter with acknowledgement of receipt addressed to the attention of the Supervisory Body, in Via Nazionale, 4/F – 24060 Casazza (BG); the report must be managed through the use of two sealed envelopes, in order to separate the identification data of the whistleblower from the report;
 1. the first with the identification data of the whistleblower together with a photocopy of the identification document;
 2. the second with the actual reportThe two envelopes must be placed inside a third sealed envelope that bears the words "reserved for the SB" on the outside.
The report will be subject to confidential registration, also by means of an independent register, by the SB.
- Verbally, by means of a statement issued and recorded in the minutes by one of the persons entitled to receive it.

In the event that the whistleblower prefers to remain anonymous, he/she may report, in addition to mode b), also through mode c) expressed above:

- By not filling in the "reporting data" section of the form,
- By not signing this form
- By not naming the sender or using a pseudonym or fictitious name.

If the report has been received by the Organisation, the Organisation will inform the whistleblower:

- That the report has been taken care of
- The possibility of being contacted to acquire further elements useful for the investigation
- The possibility of supplementing or updating the facts covered by the initial report, if additional information becomes known.

Monitoring of the functionality of the aforementioned communication channels is guaranteed by the Supervisory Body.

Important notes on how to compile and send a report (EDITOR'S NOTE)

- Law no. 179 of 30 November 2017, with the amendment of article 54-bis of Legislative Decree no. 165 of 30 March 2001, on the protection of employees or collaborators who report, provides for
- One or more channels that allow subjects...

These channels ensure the confidentiality of the whistleblower's identity in the reporting management activities

- At least one alternative reporting channel suitable to guarantee, by electronic means, the confidentiality of the identity of the whistleblower

and

Art. 3 of the RESOLUTION of 30 October 2018

"Communications and reports are submitted, as a rule, through the **IT platform form** available on the Authority's website, which uses encryption tools and guarantees the confidentiality of the identity of the whistleblower and

the content of the report as well as the related documentation" indicate **the adoption of electronic media**, which also offer advantages regarding:

- Automatic data collection
- Speed and ease of use
- Technological anonymity.

4.5 Content of reports

The whistleblower must provide all the elements necessary to allow **the Supervisory Body** to proceed with the due and appropriate checks and investigations to verify the validity of the facts being reported. The content of the reports must be accurate and consistent.

To this end, the report must contain the following elements:

- Personal details of the person making the report, with an indication of the position or function performed within the organization
- A clear and complete description of the facts reported
- Circumstances of time and place in which they were committed
- Other elements that make it possible to identify the subject(s) who have carried out the reported facts
- The indication of other subjects who may report on the facts reported
- The indication of documents that can confirm the validity of these facts
- Any other information that may provide useful feedback on the existence of the reported facts.

CHAP.5 DISSEMINATION AND TRANSPOSITION

This procedure is disseminated as widely as possible and the System Manager, **in collaboration with the Supervisory Body**, ensures:

- The availability, maintenance and updating of such documentation
- The transmission of the report form, the operating instructions and the information relating to the processing of personal data

The ALL-24.3 "Whistleblowing" **operating instructions** are sent to each member of the Organization's staff, by company email, **by the System Manager**.

In the case of new hires, the Human Resources Manager ensures that this procedure is delivered and implemented by the candidate at the time of recruitment, with the help, where appropriate, of the Head of the Function in charge.

CHAP.6 ARCHIVING AND RETENTION

In order to ensure the management and traceability of reports, the Function in charge updates.

ALL-24.2 "Whistleblowing-Register of reports" ensuring the preservation and archiving of all the related original supporting documentation relating to the reports in special paper/computer archives, with the highest standards of security/confidentiality.

In this regard, access to these documents is segregated and guaranteed by the Function itself.

The personal data collected in the context of a report are kept for the time strictly necessary for their processing, and in any case compatibly with the purpose of the processing, in compliance with the provisions of the Management System for the protection of personal data.

CHAP.7 LEGISLATIVE AND REGULATORY REFERENCES

Law no. 179 of 30 November 2017

(Provisions for the protection of those who report crimes or irregularities of which they have become aware in the context of a public or private employment relationship)

Art. Article 1 amends Article 54-bis of Legislative Decree no. 165 of 30 March 2001 on the protection of employees or collaborators who report wrongdoing and replaces it with the following:

'Article 54-bis (Protection of public employees who report wrongdoing).

1. A public servant who, in the interests of the integrity of the public administration, reports to the person responsible for the prevention of corruption and transparency referred to in Article 1, paragraph 7, of Law No 190 of 6 November 2012, or to the National Anti-Corruption Authority (ANAC), or reports to the ordinary judicial or accounting authorities, unlawful conduct of which he or she has become aware by reason of his or her employment relationship may not be sanctioned, demoted, dismissed, transferred, or subjected to any other organizational measure having a direct or indirect negative effect on the working conditions determined by the report.

The adoption of retaliatory measures, referred to in the first sentence, against the whistleblower shall in any case be communicated to ANAC by the person concerned or by the most representative trade unions in the administration in which they were implemented.

ANAC informs the Department of Public Administration of the Presidency of the Council of Ministers or the other guarantee or disciplinary bodies for the activities and any measures within its competence.

2. For the purposes of this Article, a civil servant shall mean an employee of the public authorities referred to in Article 1(2), including an employee referred to in Article 3, an employee of a public economic body or an employee of a body governed by private law subject to public control within the meaning of Article 2359 of the Civil Code.

The rules referred to in this article shall also apply to workers and collaborators of undertakings providing services and carrying out works for the benefit of the public administration.

3. The identity of the whistleblower cannot be revealed.

In criminal proceedings, the identity of the whistleblower is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.

In the context of proceedings before the Court of Auditors, the identity of the whistleblower cannot be revealed until the investigation phase has been closed.

In the context of disciplinary proceedings, the identity of the whistleblower cannot be revealed, if the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if consequent to the same.

If the complaint is based, in whole or in part, on the report and knowledge of the identity of the whistleblower is essential for the defence of the accused, the report will be usable for the purposes of disciplinary proceedings only in the presence of the whistleblower's consent to the disclosure of his identity.

4. The report shall not be subject to the access provided for in Articles 22 et seq. of Law no. 7 August 1990. 241, as amended.

5. ANAC, after consulting the Guarantor for the protection of personal data, shall adopt specific guidelines relating to the procedures for the submission and management of reports.

The guidelines provide for the use of IT methods and promote the use of encryption tools to ensure the confidentiality of the identity of the whistleblower and for the content of reports and related documentation.

6. If, as part of the investigation conducted by ANAC, it is found that discriminatory measures have been adopted by one of the public administrations or one of the entities referred to in paragraph 2, without prejudice to the other aspects of liability, ANAC shall apply an administrative fine of between €5,000 and €30,000 to the person responsible for the measure.

If it is ascertained that there are no procedures for forwarding and managing reports or that procedures do not comply with those referred to in paragraph 5, ANAC shall apply an administrative fine ranging from 10,000 to 50,000 euros to the person responsible.

If it is ascertained that the person in charge has failed to carry out verification and analysis of the reports received, an administrative fine ranging from 10,000 to 50,000 euros is applied to the person in charge.

ANAC shall determine the amount of the sanction taking into account the size of the administration or entity to which the report refers.

7. It shall be the responsibility of the public administration or the entity referred to in paragraph 2 to demonstrate that the discriminatory or retaliatory measures taken against the whistleblower are motivated by reasons unrelated to the report itself. Discriminatory or retaliatory acts taken by the administration or entity shall be null and void.

8. A whistleblower who is dismissed as a result of the report shall be reinstated in the workplace pursuant to Article 2 of Legislative Decree No 23 of 4 March 2015.

9. The protections provided for in this article shall not be guaranteed in cases in which the criminal liability of the whistleblower for the offences of slander or defamation or in any case for offences committed with the complaint referred to in paragraph 1 or his civil liability, for the same reason, is ascertained, even by a first instance judgment, in cases of intentional misconduct or gross negligence'.

Art. Article 2 of the aforementioned law: "Protection of employees or collaborators who report wrongdoing in the private sector" amends Article 6 of Legislative Decree no. 231/01 by inserting paragraph 2 after paragraph.

Paragraph 2 bis, which provides:

(a) one or more channels enabling persons who hold functions of representation, administration or management of the entity or of one of its organisational units with financial and functional autonomy, as well as persons who exercise, even de facto, the management and control of the same, and persons subject to the direction or supervision of one of the above-mentioned persons to submit, to protect the integrity of the entity, detailed reports of unlawful conduct, relevant pursuant to this decree and based on precise and consistent factual elements, or violations of the entity's organization and management model, of which they are aware by reason of the functions performed

b) at least one alternative reporting channel suitable for ensuring, by electronic means, the confidentiality of the identity of the whistleblower

(c) the prohibition of retaliatory or discriminatory acts, direct or indirect, against the reporting on the grounds directly or indirectly related to the report

d) in the disciplinary system, adopt sanctions against those who violate the measures to protect the whistleblower, as well as those who make reports with intent or gross negligence that prove to be unfounded.

Paragraph b:

The adoption of discriminatory measures against the persons who make the reports referred to in paragraph 2-bis may be reported to the National Labour Inspectorate, for the measures within its competence, not only by the whistleblower, but also by the trade union organisation indicated by the same.

Paragraph 2c:

Retaliatory or discriminatory dismissal of the reporting party is null and void. Any change of duties pursuant to Article 2103 of the Civil Code, as well as any other retaliatory or discriminatory measure taken against the whistleblower, are also null and void.

In the event of disputes relating to the imposition of disciplinary sanctions, or to demotion, dismissal, transfer, or subjection of the whistleblower to any other organisational measure having a direct or indirect negative effect

on working conditions after the report has been lodged, it shall be the employer's responsibility to demonstrate that such measures are based on reasons unrelated to the report itself.'

Art. 3 Integration of the rules on the obligation of professional secrecy, business, professional, scientific and industrial secrecy

1. In the event of a report or complaint made in the forms and within the limits set out in Article 54-bis of Legislative Decree No 165 of 30 March 2001 and Article 6 of Legislative Decree No 231 of 8 June 2001, as amended by this Law, the pursuit of the interest in the integrity of public and private administrations and in the prevention and repression of embezzlement, constitutes just cause for the disclosure of information covered by the obligation of secrecy referred to in Articles 326, 622 and 623 of the Criminal Code and Article 2105 of the Civil Code.

2. The provision referred to in paragraph 1 shall not apply where the obligation of professional secrecy is imposed on a person who has become aware of the information as a result of a professional consultancy or assistance relationship with the institution, undertaking or natural person concerned.

3. Where information and documents communicated to the body responsible for receiving them are the subject of business, professional or official secrecy, disclosure by means exceeding the purpose of eliminating the offence and, in particular, disclosure outside the communication channel specifically set up for that purpose constitutes a breach of the relevant duty of secrecy.

UNI ISO 37001:2016 (Corruption Prevention Management System)

Company Organization and Management Model

Code of Ethics for Companies

CHAP.8 ADMINISTRATIVE PENALTIES

As provided for in point 6 of Art. 54-bis, amended by Law no. 179 of 30 November 2017, if it is ascertained, as part of the investigation conducted by ANAC, the adoption of discriminatory measures by one of the public administrations or one of the entities referred to in paragraph 2, without prejudice to the other profiles of liability, ANAC shall apply a sanction to the person responsible for adopting this measure from €5,000 to €30,000.

If it is ascertained that there are no procedures for forwarding and managing reports or that procedures do not comply with those referred to in paragraph 5, ANAC shall apply an administrative fine ranging from 10,000 to 50,000 euros to the person responsible.

If it is ascertained that the person in charge has failed to carry out verification and analysis of the reports received, an administrative fine ranging from 10,000 to 50,000 euros is applied to the person in charge.

ANAC shall determine the amount of the sanction taking into account the size of the administration or entity to which the report refers.

CHAP.9 INDICATIONS AND INFORMATION FLOWS TO THE SBV

The person in charge of the Management System must communicate, within his competence and at a defined interval, the reports of non-compliance relating to the control of the Management System

Code	Description
Information 24.1	Number of non-conformities detected in the process

CHAP.10 RELATED DOCUMENTS AND FILES

Identification code	Section	Description
ALL-24.1	<i>Models</i>	Whistleblowing - Reporting violations
ALL-24.2	<i>Models</i>	Whistleblowing - Breach Reporting Register
ALL-24.3	<i>Models</i>	Whistleblowing - Instructions for reporting corrupt acts

THIS IS THE LAST PAGE OF THE DOCUMENT