GIMA S.p.A.
Via Marconi, 1
20060 Gessate (MI) – Italy
www.gimaitaly.com

ITALIAN DIVISION
gima@gimaitaly.com
EXPORT DIVISION
export@gimaitaly.com

WHISTLEBLOWING OPERATIONAL PROCEDURE

Contents

1) Introduction

This Procedure has been prepared by Gima Spa (hereinafter also the "Company") to establish and regulate internal reporting channels pursuant to the provisions set out in Legislative Decree no. 24 of 10 March 2023 (hereinafter also L.D. 24/2023 or the Decree). This Decree implementing Directive (EU) 2019/1937 applies to the protection of persons reporting violations of national laws and EU regulations and provides for the protection of individuals reporting violations of the aforementioned laws and regulations that occur within the persons' public or private work environment and are harmful to public interest or to the integrity of the public administration or the private entity.

This Procedure also complies with the regulation on the protection of personal data and, in particular, with the provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 concerning the production of natural persons with regard to the processing of personal data.

2) Reportable violations

Reportable violations include all illegal activities and instances of misconduct (of any nature, including omissions) and relevant information of which the person submitting the report has become aware in their workplace, and namely:

1. predicate offences specified in Legislative Decree 2001/23!.
2. offences committed in violation of EU legislation (listed in Annex 1 of the Decree) and pertaining to the following sectors:
   - public contracts/public procurement contracts;
   - financial services, products and markets, and prevention of money laundering and terrorist financing;
   - product safety and compliance;
   - transport safety;
   - preservation of the environment;
   - radiation protection and nuclear safety;
   - food and feed safety and animal health and welfare;
   - public health;
   - consumer protection;
   - personal privacy, personal data protection, security of information systems and networks.
3. Acts or omissions that may have adverse effects on the financial interests of the European Union;
4. Acts or omissions affecting the domestic market (e.g., violations of state subsidies and competition laws);
5. Acts or omissions that nullify the intents and purposes of the provisions set out in EU regulations.

3) Parties who may submit reports

– Employees;

- Self-employed workers;
- Collaborators, freelancers and consultants;
- Volunteers and interns;
- Shareholders with administrative, management, supervisory or representative functions;
- Workers or collaborators who work for entities that supply goods or services or construction works to the Company (e.g., suppliers or contractors).

Reports may also be submitted by persons in the following circumstances:

- During the employment relationship
- During the hiring phase;
- During the probation period;
- After the conclusion of the employment relationship, provided that the information was acquired before the termination of their employment.

4) Internal reporting channels provided by the Company

Pursuant to the Decree, the Company has duly established written and verbal channels as detailed below:

1. Wallbreakers software platform
2. Email box and voicemail
3. Face-to-face meeting with the whistleblower

Wallbreakers software platform (written channel)

The main steps to be followed by a whistleblower are:

- Enter the company website and select the whistleblowing section (link to website: https://gima.wallbreakers.it/).
- In the whistleblowing section, select the "New Report" button. This opens a popup with the terms of use of the platform, the relevant policy and this procedure.
- Agree to the aforementioned terms to open a page where the whistleblower can select. type of violation (e.g., violations of Model 231, the EU Regulation, etc.).
- Selecting the type of violation opens a questionnaire where the whistleblower can enter all the information needed to provide as much detail as possible about the report; at this point, the whistleblower may decide not to disclose their identity (and submit an anonymous report using a specific feature provided by the software).

- Provide a detailed description of time and place and the information need to identify the person to whom the contested facts are to be attributed.
- At the end of this phase, the Whistleblowing Report Manager acknowledges receipt of the report, and the software provides the whistleblower with a code that enables them to access their report and monitor its status (e.g., check for requests from the Report Manager, response, outcomes communicated by the latter).
- Save and store the code received to be able to track the status of their report. If a code is lost or forgotten, it cannot be recovered.

Voicemail

- Record the voice message by connecting to the audio of their PC/telephone/tablet.
- The message is handled by the platform and made available to the person receiving the report. The whistleblower is given a code they can input into the platform to track the progress of their report.

Face-to-face-meetings with a whistleblower

Whistleblowers can request a face-to-face meeting with the person, the office or the external party who manages the reports.

The Report Manager shall arrange a meeting with the whistleblower within a maximum of 15 days from the date of the request. With the consent of the whistleblower, the Report Manager may record the meeting using appropriate storage and playback devices.

If the whistleblower does not consent to the recording or the Report Manager does not have an appropriate recording device, the latter shall draw up a report to be signed by the whistleblower. A copy of this report shall be given to the whistleblower.

If the management of reports has been entrusted to an external party, it is advisable to hold the meeting at the company premises of the latter.

All the documentation and the recording of the meeting are stored and filed in lockable cabinets that can only be accessed by the Report Manager.

5) The Report Manager

The Company has established a committee and entrusted it with the role of Report Manager:

The committee is composed as follows:

Ms Fiorenza Messina, HR Manager at GIMA

Mr Fabio Pusineri, ICT Manager at GIMA

Barbara Passanisi, legal counsel for Gima

6) Internal report management actions – Preliminary examination

Upon receiving a report, the Report Manager undertakes the following actions:

1. issues the whistleblower an acknowledgement of receipt within seven days of receipt;
2. carries out a preliminary examination of the content of the report by verifying the subjective and/or objective grounds for the report (whether the whistleblower has standing to make the report and/or whether the report concerns one of the areas of application of the Decree) and, based on the Decree, assesses the admissibility of the report (detailed description of time and place and information to identify the person to whom the alleged facts are attributed);
3. based on the assessments described above, the Report Manager archives the reports that are deemed inadmissible and/or do not meet the subjective and/or objective requirements, and, in particular, are deficient in terms of:
   - Lack of essential elements substantiating the violation;
   - Facts of the violation manifestly lacking the foundations specified by the Legislator and the Decree;
   - Facts reported in a generic and approximate manner that does not lead to an understanding of the alleged violation, even after specific requests for additional information from the Report Manager;
   - Violations reported by attaching irrelevant or inappropriate documentation that does not lead to an understanding of the content of the report;
   - Submission of documentation without an actual report of a violation.

In the latter case, the Report Manager is required to detail (through the channel used by the whistleblower) the reasons and motivations for closing the case.
A report that is anonymous but is accurate, detailed, and supported by appropriate documentation is handled as a regular report and according to this procedure.

7) Internal report management actions – Preliminary investigation

At the end of the preliminary examination, in cases other than dismissal, the Report Manager takes charge of the report and carries out the following activities:

- maintain communication with the whistleblower through the channel chosen by the latter and, where necessary, request additional information;
- carry out the necessary checks, analyses and assessments on the validity of the reported facts, also for the purpose of formulating and/or recommending any corrective actions with a view to strengthening the Company's internal control system;
- engage experts with appropriate technical and professional skills and schedule hearings with internal or external individuals as deemed necessary;
- diligently follow up on the report and respond to it within three months of the date of notification of receipt, or, in the absence of such notification, within three months of the expiry date of the seven-day time limit following the date of submission of the report.

Before proceeding with any action (relating to the management of reports received via the aforementioned channels), the Report Manager shall obtain the explicit consent of the whistleblower through an ad hoc form in the following cases:

- to be authorised to disclose personal data relating to the identity of the whistleblower and/or sensitive data contained in a report when other parties (internal or external parties, experts, and/or the Supervisory Body) have to be involved in the management of the report and in conducting assessment, preliminary examination and preliminary inquiry activities;
- when the disclosure of the aforementioned data is essential for the defence of the party accused of wrongdoing, when the accusation is based, in whole or in part, on the report.

In such cases, the company functions and/or the external parties involved are subject to the same confidentiality obligations that apply to the Report Manager pursuant to the Decree.
If the whistleblower does not give their consent and whenever it is strictly necessary, the Report Manager obscures the personal data contained in the report prior to sharing the report with company functions and/or external parties.

8) Internal report management actions – Response to the whistleblower

Once the investigation has been completed, the Report Manager is required to respond to the whistleblower -- within three months of the expiry date of the seven-day time limit following the date of notification of receipt of the report, communicating one of the following outcomes:

1. Motivated dismissal (see Section 6 "Internal report management actions – Preliminary examination");
2. Following a positive assessment of its soundness, the report has been forwarded to the competent authorities;
3. Activities carried out up to the end of the 3-month period and/or the activities that the Report Manager intends to carry out.

The retention period for the reports and related documentation attached thereto is expressly determined pursuant to Article 14 of the Decree: *"Internal and external reports and related documentation shall be retained for the time necessary to process the report and in any event for no longer than five years from the date of notification of the final outcome of the reporting procedure"*. Once the aforementioned time limits have expired, the report and the personal data contained therein shall be destroyed or anonymised, in accordance with the technical deletion and backup procedures.

9) External reporting channel

A whistleblower can submit a report via the external channel activated by ANAC when the conditions listed below are satisfied:

- The whistleblower has already submitted an internal report without receiving any response from the Report Manager;
- The whistleblower has substantiated grounds to believe that, if they were to submitted an internal report, it would not be followed up effectively or the report could result in retaliation against them;
- The whistleblower has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to public interest.

Reports can be submitted through the ANAC platform at the following address: https://www.anticorruzione.it/-/whistleblowing or through the modalities detailed by ANAC on their website https://www.anticorruzione.it/

10) Public disclosure

For the purposes of this Procedure, by public disclosure it is meant making information about violations available to the public at large through the press or electronic media or by any other means of dissemination that can reach a large number of people.

Whistleblowers making a public disclosure are entitled to the protection provided for in the Decree provided that, at the time of public disclosure, one of the following conditions is met:

- The whistleblower has previously used internal and external reporting channels, or has directly filed an external report under the conditions and according to the modalities specified in the Decree and in the previous Section, and no response was provided within the established time limits;
- The whistleblower has reasonable grounds to believe that the violation may pose an imminent or manifest danger to public interest;
- The whistleblower reasonably believes that an external report may entail a risk of retaliation or may be ineffective on account of the specific circumstances of the case in question;
- The whistleblower has well-founded reasons to believe that the evidence and the documents submitted with the report may be concealed or destroyed, or has grounds to believe that the individual receiving the report may be colluding with the perpetrator of the violation or even be directly involved in the violation.

11) Prohibition of retaliation

Whistleblowers shall not be subject to retaliation by the Company for having submitted a report in accordance with this Procedure and on the basis of the Decree.

By retaliation it is meant the actions taken by a company upon receiving a report under the circumstances described above, which, by way of exemplification, may include:

- dismissal, suspension or equivalent measures;
- demotion or denial of promotion;
- change in job duties, change of workplace, reduction in salary, change in working hours;
- suspension of training or restrictions on access to training;
- unfair performance evaluations or unfavourable references;
- disciplinary measures or other sanctions, including financial ones;
- coercion, intimidation, harassment or bullying;
- discrimination or any form of unfavourable treatment;
- non-conversion of a fixed-term employment contract to a permanent employment contract, where the worker has a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;

- damage, also in terms of personal reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
- inclusion in blacklists based on formal or informal agreements for the sector or industry that may make it impossible for the whistleblower to find employment in the field in future;
- early termination or cancellation of a contract for the supply or goods or services;
- cancellation of a licence or a permit;
- requests to subject the whistleblower to psychiatric or medical examinations.

12) Protective measures

The Decree defines the following measures for the protection of whistleblowers and any persons who have helped them submit a report (e.g., facilitators):

- prohibition of retaliation following the submission of a report;
- measures providing support in the form of free assistance and advice from third-party organisations listed on the ANAC website with regard to reporting procedures and regulatory provisions in favour of whistleblowers and other persons involved.

A whistleblower who has been subjected to retaliatory measures may:

- send and/or submit a communication to ANAC indicating the retaliation measures they believe they have been subjected to as a result of their report;
- assert in court the nullity of all retaliatory acts they believe they have suffered as a consequence of their report.

Protective measures also apply to parties, other than the whistleblower, who may be subjected to retaliation on account of the role played or their close relationships or connections with the whistleblower; in particular, the measures apply the following persons/entities:

- The Facilitator: a person who assists the whistleblower with the reporting process, works in the same work context, and whose assistance should remain confidential.
- Persons in the same workplace: individuals who, besides working in the same company as the whistleblower, are connected to the latter by stable emotional links or by family relationships within the fourth degree.
- Work colleagues: individuals in the same work context as the whistleblower who have a regular and ongoing working relationship with the latter.
- Legal entities either wholly or majority-owned, including through third parties, by the whistleblower.
- Entities the whistleblower works for.

13) Conditions for the protection of whistleblowers

- At the time of submitting their report, or filing an accusation with a Judicial Authority, the whistleblower had reasonable grounds to believe that the information on the violations reported, publicly disclosed or denounced was true and that the violation came within the scope of the misconduct sanctioned by the Decree.

– The report or disclosure was made in accordance with the provisions set out in the Decree.

The protective measures also apply in the case of anonymous reports and when a whistleblower is subsequently identified and is subjected to retaliation.

14) Limitation of whistleblower liability

A whistleblower is immune from civil, criminal and administrative liability in the following situations:

- dissemination and use of information covered by official secrecy (Article 326 of the Italian Criminal Code);
- disclosure of professional secrets (Article 622 of the Italian Criminal Code)
- disclosure of scientific or industrial secrets (Article 626 of the Italian Criminal Code)
- breaches of the duty of fidelity and loyalty (Article 2015 of the Italian Civil Code)
- copyright infringements
- breaches of personal data protection provisions
- the act of disclosing or disseminating information that damages the reputation of the person involved or reported

This limitation of liability only applies provided that, at the time of the disclosure or dissemination, the whistleblower has reasonable grounds to believe that the disclosure or dissemination of the information is necessary to reveal the violation, or provided that the reporting, public disclosure, or notification to the competent authorities is made in accordance with the conditions set out above in Section "13) Conditions for the protection of whistleblowers".

Moreover, unless doing so is a criminal offence per se, a whistleblower does not incur any liability, including liability of a civil or an administrative nature, for acquiring information about violations or for accessing such information.

Criminal liability, as well as any other liability, including liability that falls under civil or administrative laws, is not ruled out, however, for behaviours, acts or omissions that are not related to the submission of a report, the filing of an accusation with judicial or with accounting authorities, disclosure to the public, or that are not strictly necessary to reveal the violation.

15) Loss of protection

Protective measures no longer apply it is ascertained, including by a first instance ruling, that the whistleblower has incurred criminal liability for defamation or slander, or civil liability in cases of fraud or gross negligence.

16) Penalties

ANAC makes a distinction between natural persons (individuals) and legal persons (entities like corporations) responsible for, and/or recipient of, a penalty for violation of the provisions of the Decree.

The liability for retaliatory acts will always fall on the person who has engaged (or even just suggested or proposed) such acts.

Accordingly, ANAC imposes penalties pursuant to the terms and conditions set out below:

- from €10,000 to €50,000 when it ascertains that the natural person identified as liable has committed acts of retaliation;

- from €10,000 to €50,000 when it ascertains that the natural person identified as liable obstructed the reporting or attempted to do so;
- from €10,000 to €50,000 when it ascertains that the natural person identified as liable has violated the confidentiality obligation as per Article 12 of the Decree. This is without prejudice to the penalties applicable by the Data Protection Authority for matters falling within its area of control under the regulations on personal data;
- from €10,000 to €50,000 when it ascertains that no reporting channels have been established. In this case, the liability falls on the governing body of the Company;
- from €10,000 to €50,000 when it ascertains that no procedures have been adopted for the implementation and management of reports or that the procedures adopted do not comply with the provisions of the Decree. In this case, the governing body of the Company is held liable;
- from €10,000 to €50,000 when it ascertains that the reports received have not undergone the required checks and analyses. In this case, the Report Manager is held liable (besides such penalties, the disciplinary actions provided for in the applicable national collective agreement may also be imposed, where applicable);
- from €500 to €2,500 when the whistleblower has been found liable for defamation or slander in cases of fraud or gross negligence, even by a first instance ruling, unless the whistleblower has already been convicted, including at the first instance level, for the offences of defamation or slander or for having committed the said offences in the act of filing the accusation with the judicial authorities.

17) Confidentiality obligations with regard to the identity of the whistleblower

The Decree and this Procedure impose on the Manager a confidentiality obligation encompassing any information contained in a whistleblower's report from which the identity of the latter could be inferred either directly or indirectly (as well as the identity of other persons involved and/or mentioned in the report and the identity of facilitators). Without the express consent of the Whistleblower, this information cannot be disclosed to persons other than the Report Manager expressly authorised to process such data and information in accordance with Articles 29 and 32(4) of the GDPR and Article 2-quaterdecies of the Italian Privacy Code.

18) Processing of personal data and the GDPR

The Company processes personal data collected for the purpose of managing the reports coming in through internal reporting channels in accordance with Regulation (EU) 2016/679 (GDPR) and the applicable Italian Personal Data Protection Code.
In this connection, the Company has proceeded to:

- Issue this Internal Procedure on the use of reporting channels and the conditions for submitting reports, via both internal and external channels, in the instances provided for by the whistleblowing legislation (subjective scope of application, Article 2 of the Decree), and the identity of the person, internal office or external entity responsible for managing the reports.
- Update its Privacy Policy and Data Processing Register.

- Update, implement and integrate the document on security measures with the provisions set out in Article 32 of the GDPR, identifying technical and organisational measures suitable to ensure a level of security appropriate to the specific risks arising from processing activities, based on a data protection impact assessment carried out pursuant to Article 35 of the GDPR.
- Define the information to be provided to the data subject pursuant to Articles 13 and 14 of the GDPR.
- Provide for specific data processing authorisations for the person or internal office responsible for receiving the reports pursuant to Articles 29 and 32 of the GDPR and Article 2-quaterdecies of the Privacy Code.
- Appoint an external Data Processor, in accordance with Article 28 of the GDPR, from the external company that supplies the software and/or is responsible for receiving the reports.

The person reported (i.e., the author of the alleged violation) is not entitled to exercising the rights provided for in Articles 15 to 22 of the GDPR (by contacting the Data Controller or by lodging a complaint with the Data Protection Authority pursuant to Article 77 of the GDPR) if doing so would cause effective, concrete and significant prejudice to the confidentiality of a whistleblower's identity (Article 2-undecies, letter f) of the Privacy Code and Article 23 of the GDPR) and/or the pursuit of compliance with the regulatory provisions contained in the Decree. The persons responsible for assessing the request submitted by the person reported (i.e., the author of the alleged violation) must evaluate and/or balance the need to protect the rights of individuals with the need to combat and prevent violations of the rules of good corporate governance and the applicable regulations.

19) Making this Procedure known and final provisions

This Procedure has been adopted by the Company's Board of Directors in accordance with internal rules and practices and may be updated pursuant to the same internal rules and practices.

This Procedure and the modalities of access to internal channels and all information of use relating to the Decree are available for consultation at the Company premises and are published in a dedicated section of the company website https://www.gimaitaly.com/
The Procedure and all related and relevant information are also made available to new hires.
Training on whistleblowing and the contents of this Procedure has been included in the employee training plans organised by the Company.

Gessate, 11 December 2023

Gima Spa