Lombardi

ORGANISATIONAL ACT FOR THE IMPLEMENTATION OF THE WHISTLEBLOWING REGULATION

(Legislative Decree No. 24 of March 10th, 2023)

Approved by Board of Directors on

December 15th, 2023

Updated on April 18th, 2025

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

1. FOREWORD

1.1 Whistleblowing: legal basis and nature of the institution

Legislative Decree No. 24 of March 10th, 2023 (hereinafter also referred to as the Whistleblowing Decree or simply the Decree), which came into force on March 30th, 2023, implements EU Directive 2019/1937 concerning the protection of so-called Whistleblowers (or "informants"). These are individuals who report, depending on the case and as will be further clarified below, violations of national or European Union laws that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a work-related context.

This directive introduced, for all Member States, a genuine right to report violations.

Legislative Decree No. 24 of 2023 consolidates into a single legal text the entire framework governing internal and external reporting channels, as well as other forms of reporting and the system of protections afforded to whistleblowers (and to other individuals expressly identified by the legislator), both in the public and private sectors. This results in a comprehensive and uniform legal framework aimed at enhancing the protection of whistleblowers, ensuring they have the necessary tools to contribute to the disclosure of relevant violations, and are informed from the outset of the rights and duties that are essential for fulfilling the purpose of the legislation.

Considering the Company's adoption of the Organization and Management Model pursuant to Legislative Decree No. 231 of 2001 (hereinafter also referred to as the 231 Model or MOGC 231), any violations relevant under that regulation or of the procedures forming part of the Model itself may also be subject to reporting under this Organisational Act and, where the conditions established by Legislative Decree No. 24 of 2023 are met, will be covered by the same protections and safeguards.

The current regulation aims to encourage the disclosure and prevention of risks and situations that may be detrimental to the public and private entities concerned and – indirectly – to the collective public interest.

This objective is pursued by fostering cooperation among those who operate or have operated within public or private work environments, through the strengthening of the protection system established in their favor, both in terms of confidentiality and in cases of retaliation.

1.2 Purpose of the document and summary of contents

The Company is committed to promoting a corporate culture based on ethical behaviour and an efficient system of corporate governance.

The Company operates in full compliance with all applicable supranational, national, and local laws and regulations, and expects the same level of diligence from all its personnel and third parties with whom it interacts during its business activities.

For these reasons, the Company recognizes the importance of defining, within this Organisational Act, the procedures that govern the entire process of submission, receipt, analysis, and management of reports concerning violations relevant under Legislative Decree No. 24 of 2023. The aim is to promote a corporate environment in which senior management, employees, and third parties have the tools to assess the significance of observed conduct and, where appropriate, feel comfortable submitting such reports. The Company believes that collaboration among all those involved in corporate dynamics is essential to achieving the highest standards of efficiency and legality.

This Organisational Act forms an integral part of the Organization, Management and Control Model pursuant to Legislative Decree No. 231 of 2001 (see Annex 4 of the Model).

1.3 Recipients

The recipients of the provisions contained in this Organisational Act are identified as the following parties:

- the shareholders;
- individuals who hold roles of representation, administration, or management within the Company, including those who effectively manage and control it;
- employees;
- partners, clients, suppliers, consultants, collaborators (including volunteers and/or interns), and more generally, anyone who has an interest-based relationship with the Company (so-called “third parties”).

According to the Whistleblowing Decree, the term whistleblower refers to “*a natural person who reports or publicly discloses information on violations acquired in the context of their work-related activities*”.

1.4 Subject of the report

A report refers to the written or oral communication of information regarding violations relevant under the Whistleblowing Decree, which occurred in the course of work activities or that have a direct or indirect impact on such activities, and that cause or may cause harm or detriment to the Company, its employees, or third parties.

The report may concern information, including founded suspicions, regarding:

1) violations of EU law and all national provisions implementing the areas listed in Annex 1 of Legislative Decree No. 24 of 2023. These specifically include the following sectors: public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection; network and information system security;

2) acts or omissions affecting the financial interests of the EU (Art. 325 of the Treaty on the Functioning of the EU, regarding the fight against fraud and illegal activities affecting the EU's financial interests), as identified in EU regulations, directives, decisions, recommendations, and opinions. This includes fraud, corruption, and any other unlawful activity related to EU expenditures;

3) acts or omissions affecting the internal market, which undermine the free movement of goods, people, services, and capital (art. 26, paragr. 2, of the Treaty on the Functioning of the EU). This includes violations of EU competition and state aid rules, corporate tax violations, and mechanisms designed to gain a tax advantage that defeats the purpose of applicable tax laws;

4) acts or conduct that frustrate the purpose or intent of the provisions of EU law in the sectors indicated above;

5) unlawful conduct relevant under Legislative Decree No. 231 of 2001 and violations of the 231 Model (MOGC 231).

The above violations may consist of any measure, conduct, act, or omission carried out in the context of work activities or having a direct or indirect impact on them, that causes or may cause harm or detriment to the Company, its employees, or third parties.

Reports about violations may also concern not yet committed violations, which the whistleblower reasonably believes may occur based on concrete, precise, and consistent elements, as well as any conduct intended to conceal such violations.

Reports can be made not only during one of the legal relationships identified in the previous paragraph, but also, pursuant to Art. 3, para. 4 of Legislative Decree No. 24 of 2023:

a) before the legal relationship has started, if the information on the violations was obtained during the selection process or other pre-contractual phases;

b) during a probationary period;

c) after the termination of the legal relationship, if the information on the violations was obtained before its conclusion.

The following situations do not constitute a report relevant under the Whistleblowing Decree and, as such, they are not subject to the protections and guarantees it provides:

1) disputes, claims, demands, or communications related to the whistleblower's personal interest, involving individual employment relationships (it should be noted, however, that the motives behind a report do not affect its handling or the application of the protections provided by the Decree);

2) matters related to national defence and security;

3) violations concerning specific sectors already mandatorily regulated by EU acts or their national implementing provisions, or directly by national acts listed in Part II of the Annex to Legislative Decree No. 24 of 2023 (e.g., financial services, anti-money laundering, terrorism, transport safety, environmental protection);

4) unfounded information, already fully public, or mere rumours or hearsay.

2. REPORTING CHANNELS

2.1 Internal reporting channels

Internal reporting channels represent the preferred means for communicating information about potentially relevant violations, as they are closer to the origin of the matters being reported.

In accordance with the provisions of the Whistleblowing Decree and the Guidelines issued by ANAC on the subject, the Company has activated and made available to the intended recipients an internal digital channel for submitting reports.

The information channel is cons

This digital channel consists of a dedicated web portal, accessible at the address https://lombardigroup.wbisweb.it (hereinafter referred to as the Whistleblowing Portal or simply the Portal). The Portal is managed by ISWEB S.p.A., a company that has certified its technical and regulatory compliance and has been appointed as Data Processor for the entrusted activities (**see annexes 1a–1b–1c**).

Upon accessing the Portal, the whistleblower will be briefly and clearly informed again about the key features of the tool.

By clicking on the "*Submit a Report*" button – after having read and accepted the information notices regarding the purpose of the applicable legal framework and the processing of personal data – the whistleblower can submit a report using one of the following methods:

- written communication, by completing the form provided, which requires the indication of relevant circumstances for a complete description of the reported violation (e.g., reporter's statement, type of reported conduct, time and place of occurrence, duration of the conduct, individuals involved in any capacity, description of the facts, as well as any other information deemed useful for verifying the report, including mention of any other parties who were previously informed of the same facts, such as authorities and/or institutions. For a more detailed overview of the form's contents, see the attached form, **annex 2**);
- Oral communication, by uploading an audio file to the Portal containing a full description of the reported violation. This can be done – after completing the above-mentioned form (see **annex 2**) – using the "upload" button located in the "attachments" section of the Portal (this section may also be used in conjunction with the written report to provide supporting documentation, of any format or type, to substantiate the reported facts). Regarding the content of the oral communication recorded in the audio file, if the form completed in the initial sections of the Portal is summarized, incomplete, and/or does not contain the required information, the whistleblower is encouraged to include in the audio file all the data referenced in the form, in order to ensure complete identification of the reported violation and the involved individuals;
- Request for a meeting with the Manager responsible for handling the internal reporting channel (hereinafter, also referred to simply as the Reporting Manager or Manager) to orally communicate the report in person: If the whistleblower chooses this method, it will still be necessary to fill in the mandatory sections of the form as indicated on the Portal (see **annex 2**) and accept the terms of service detailed below, until the submission process is complete. In the "*Description of the facts*" section, the following phrase must be included: "*I intend to request a meeting with the Manager responsible for the internal reporting channel within a reasonable timeframe in order to orally report the whistleblowing violation I have become aware of in the course of my professional activity*". (Should the whistleblower choose one of the first two reporting methods, they may still request an in-person meeting with the Reporting Manager after submission, in accordance with the procedures described in more detail below).

Regardless of the reporting method chosen by the whistleblower, by following the operational steps provided by the Portal, the whistleblower will access the section titled "*Identity*", where they can choose either to enter their personal details or to proceed with completing and submitting the report anonymously (an anonymous report is one in which the whistleblower's identity cannot be determined).

In the first case, through the encryption tools built into the Portal, the whistleblower's identity will be known only to the Reporting Manager, who – in accordance with the Whistleblowing Decree – is obligated to ensure its confidentiality and may disclose it only if absolutely necessary and with the whistleblower's explicit consent, or in the case of involvement of the competent Authorities and upon their explicit request.

In the second case, it is understood that the choice to remain anonymous may later be changed by the whistleblower through the functions available on the Portal itself—first and foremost, the so-called "chat" (the section titled "comments"), which, as will be explained, allows for the exchange of information between the whistleblower and the Reporting Manager via a messaging service after the report has been submitted. The report can still be submitted and, along with any attached documentation, will be archived and managed by the Manager appointed by the Company, provided it is sufficiently detailed and suitable to allow the Manager to carry out the necessary verification process.

In fact, while the legislation mandates confidentiality rather than anonymity, the Company—seeking to promote by every available means the spirit of cooperation encouraged by the Whistleblowing Decree, and to effectively verify any alleged violation within its working environment or in a related context—establishes through this Organisational Document that anonymous reports, if adequately detailed, shall be treated the same as ordinary reports and thus subjected to the same verification procedure. At the same time, whistleblowers are reminded of their duties and responsibilities, as set forth by the legislator, regarding the truthfulness of the information on which the report is based.

After completing the "*identity*" section, the Portal will allow the whistleblower to access the area called "*attachments*", where they can upload any documentary evidence deemed relevant to substantiate one or more aspects of the reported violation. Using the "*upload*" button, the whistleblower may attach documents and/or multimedia files considered useful for assessing the validity of the reported violation. (While uploading attachments is optional, it is strongly recommended whether the whistleblower possesses such evidence, in order to facilitate the verification process carried out by the Reporting Manager). In the case of oral communication, the whistleblower may use this Portal feature to upload the audio file containing the recording of their report, following the previously provided instructions.

Once any attachments have been uploaded, the Portal will guide the whistleblower to a new section called "*additional information*", where—by answering the questions in the form (see **annex 2**)—they can provide further details regarding the report. This includes the possible indication of the so-called "facilitator", i.e., the person who, operating within the same work context as the whistleblower, assisted in reporting the violation (a person to whom, as will be discussed, specific protections are extended).

Once this section has also been completed, the whistleblower will access the final operational step provided by the portal. In this step—after reading and accepting the terms of service, of which this Organisational Act and the related privacy notice form an integral part—they will be able to submit the report by clicking the "*submit*" button.

By doing so, the reporting procedure will be completed through the transmission of its content exclusively to the Reporting Manager, and the platform will generate a unique, sequential identification code called the "*key code*".

This code must be securely stored and kept by the whistleblower, who is the only person to have actual knowledge of it. It will allow them—by returning to Portal's website (https://lombardigroup.wbisweb.it) and entering it in the section "*Have you already submitted a report*? *Enter your receipt*"—to access their report area, check the status of its management, and interact via the so-called "chat" with the Reporting Manager. This includes providing additional information and/or documentation or requesting a dedicated meeting with the Manager for this purpose. Similarly, the Reporting Manager may use the same tool for the same purposes.

In case of loss, the "*key code*" cannot be recovered in any way. In such an event, the whistleblower—if they wish to continue receiving updates on the report's status or submit any additional information—must initiate a new reporting procedure by answering "yes" to the question "*Have you already submitted a report but lost your key code?",* which appears at the beginning of the section titled "*report*". In the subsequent information fields, they must provide all the necessary details to enable the Reporting Manager to associate the new report with the one previously submitted.

2.2 Management of internal reports

The Company has entrusted the management of the internal whistleblowing channel to the Supervisory Body appointed pursuant to Legislative Decree No. 231/2001 (hereinafter also referred to as the "OdV" from the Italian word "*Organismo di Vigilanza*"). Based on its specific and proven professional expertise, the OdV has been formally assigned the role of Manager of the internal whistleblowing channel and, for privacy purposes, designated as the authorized party for processing the data contained in the reports.

The aforementioned Manager shall be the only person authorized to access the content of reports submitted through the internal whistleblowing channel, via the section of the Whistleblowing Portal reserved for this purpose. Access is granted through authentication credentials used exclusively by each member of the Supervisory Body (OdV), with activity tracking for each individual member.

When a report is submitted via the Portal, or an existing report is updated through the same digital platform, the Portal will automatically generate a notification—devoid of specific content and/or any data related to the report—which will be sent to the email addresses indicated and exclusively used by each member of the OdV. This allows them to access their reserved area of the Portal, review the content of the report, and fulfill the obligations established by the Decree.

All reports will be handled by the Reporting Manager fairly and impartially, with utmost care and in full compliance with all requirements, technical and operational procedures, guarantees, and safeguards set out by the Decree.

In the event of a report received via the Portal, the Reporting Manager is required to carry out the following actions:

- Issue an acknowledgment of receipt to the whistleblower within 7 days of the date of receipt. Technically, in order to ensure maximum confidentiality of the whistleblower's identity, the Portal does not allow for a direct notification to be sent. However, the whistleblower can verify the actual receipt of the report by accessing their reserved area using the "key code" received at the time of submission and viewing the status of the report. Until the Reporting Manager accesses their reserved area of the Portal, the report status will appear as "*new*". Upon the Manager's first access and formal review of the report's content, the Portal will automatically change the status from "*new*" to "*open*," with no possibility for the Manager to revert it to its initial state. As the handling process advances, the Manager may update the status only progressively, up to the final "*closed*" status, allowing the whistleblower to remain continuously informed. The change in status from "*new*" to "*open*," along with the date and time of the last update (automatically registered by the Portal), shall be considered for all purposes as the formal "acknowledgment of receipt";
- In the case of an oral report made during an in-person meeting requested by the whistleblower, and subject to their express consent, document the report either through an audio recording using a device suitable for storing and listening, or by drafting written minutes. If minutes are drafted, the whistleblower must be allowed to review, correct, and confirm the content by signing the document;
- Maintain communication with the whistleblower, requesting—if necessary—clarifications and/or additional documentation through the dedicated area of the Portal;
- Duly and effectively follow up on the reports received;
- Provide feedback to the whistleblower within 3 months from the date of acknowledgment of receipt or, in the absence of such acknowledgment, within 3 months from the expiration of the 7-day deadline following the submission of the report.

By proper and effective follow-up is meant, first and foremost, compliance with reasonable timeframes and the need to ensure the confidentiality of the data involved.

The Reporting Manager will also be required to conduct a preliminary assessment to verify whether the report meets the essential requirements for admissibility, in order to grant the whistleblower, the protections provided by law that will be explained in this document.

For the evaluation of these requirements, the Manager will refer to the criteria outlined by ANAC in the Guidelines of July 12th, 2023, and any subsequent updates and/or amendments.

In particular, the Manager will be required to declare:

- the unfounded nature of the report due to the lack of factual elements sufficient to justify an investigation;
- the non-specific content of the report when it is not possible to understand the facts to which it refers or if the report is accompanied by inappropriate or irrelevant documentation.

Once the report has been assessed as admissible under the Whistleblowing Decree, the Manager will initiate an internal investigation into the reported facts or conduct, to verify their actual substance.

To carry out the investigation, the Manager may engage in a dialogue with the whistleblower, requesting clarifications, documents, or additional information, either through the Portal or in person. Where necessary, the Manager may also obtain documents and records from other company departments, rely on their support, or involve third parties, including consultants, through interviews or other inquiries—always ensuring that the confidentiality of the whistleblower, the reported individual, any other person mentioned and the contents of the report is not compromised.

At the conclusion of the investigation, the Manager will provide feedback to the whistleblower.

If, based on the findings, the report is deemed manifestly unfounded, it will be formally closed with appropriate justification.

If, on the other hand, the report appears to be founded, the Manager must promptly notify the relevant internal bodies of the Company (including disciplinary matters), or external authorities and institutions, each according to their respective areas of responsibility, depending on the subject and outcome of the report.

If it is ultimately determined that the report was made in bad faith, the Reporting Manager shall immediately inform the Company’s administrative body so that appropriate actions may be taken to hold the whistleblower accountable, both from a disciplinary standpoint and before the competent Authorities.

The Reporting Manager is not responsible for determining individual liability, regardless of its nature, nor for carrying out legitimacy or merit reviews of acts and decisions adopted by the entity/administration being reported.

Regarding the "*feedback*" to be provided within the 3-month deadline, it is noted that such feedback may consist of communication of the report's dismissal, launch of an internal investigation and possibly its results, measures taken to address the reported issue or referral to a competent Authority for further investigation.

The same feedback may also be preliminary or partial, meaning it may contain information on the actions being undertaken, as well as the status of the ongoing investigation. In such cases, the outcome of the investigation must still be communicated to the whistleblower once completed.

If, due to an error and/or negligence on the part of the whistleblower, a report concerning violations relevant under the Whistleblowing Decree is submitted within the Company through any means other than the designated internal reporting channel, and using methods not technically supported by the Portal, the individual or Company function who becomes aware of the report and its contents—provided the whistleblower has explicitly stated their intention to benefit from whistleblowing protections, or such intention is clearly inferred from the report—must comply with the same confidentiality obligations imposed on the Reporting Manager.

In such cases, the report and any attached documents/files must be submitted to the Reporting Manager via the Whistleblowing Portal within 7 days of receipt, by initiating and completing the standard reporting procedure. If possible, the whistleblower should be informed at the same time.

Otherwise, the report will be handled as an ordinary report and therefore will not be subject to the protections and safeguards provided by the Decree.

2.3 External reporting channels

An external report refers to "*the written or oral communication of information concerning violations, submitted through the external reporting channel referred to in Article 7*".

External reports can only be submitted by individuals listed under Article 3 of the Whistleblowing Decree (bearing in mind that the whistleblower, as previously defined, refers to the natural person[1]

[1] Reports submitted by other parties — including representatives of trade unions — shall not be taken into consideration, as the whistleblowing mechanism is intended to protect the individual natural person acting in their own name and on their own behalf, and not on behalf of a trade union or under its designation.

who submits the report — namely, those already mentioned in paragraph 1.3 “Recipients” in relation to internal reporting).

While internal channels are preferred, Legislative Decree No. 24 of 2023 allows for the possibility of using external reporting channels, provided that the conditions expressly laid out in Article 6 are met.

Specifically, a whistleblower may file an external report if, at the time of its submission:

- the internal channel, although mandatory, is not active, or, even if active, does not comply with the Decree's requirements regarding the procedures for submitting internal reports, the individuals authorized to handle them, and the protective system and safeguards that must be effectively ensured;
- the whistleblower has already submitted an internal report which has not been taken into account yet by the designated person or office (this refers to cases where the internal channel has been used but failed to function properly — i.e., the report was not processed within a reasonable time or no action was taken to address the violation);
- the whistleblower has reasonable grounds, based on concrete circumstances and verifiable information (not mere assumptions), to believe that submitting an internal report would:
  - not be effectively followed up (e.g., if the person ultimately responsible in the work context is involved in the violation, or there is a risk that the violation or evidence may be concealed or destroyed, or the effectiveness of any investigation by the competent authorities could otherwise be compromised, or if ANAC is deemed more suitable to handle the violation, especially in areas under its direct jurisdiction);
  - expose the whistleblower to a risk of retaliation (including through breaches of confidentiality regarding their identity);
  - concern a violation that may pose an imminent or obvious danger to public interest (e.g., requiring urgent action to safeguard human health and safety or to protect the environment).

The management of external reporting channels is the exclusive responsibility of ANAC (the National Anti-Corruption Authority).

At present, ANAC has activated the following external reporting channels:

- online platform (written communication);
- telephone service with an operator (oral communication);
- request to schedule a face-to-face meeting to orally report the external disclosure.

For a comprehensive overview of the procedures for submitting and handling external reports, please refer to the specific section of the ANAC Guidelines dated July 12th, 2023, as well as any subsequent amendments or additions.

Finally, as will be more specifically detailed in the section regarding protections, pursuant to Article 19 of Legislative Decree No. 24 of 2023, the whistleblower and the other parties referred to in Article 3, paragraph 5, may report to ANAC — via the online platform — any retaliatory measures they believe they have suffered as a result of the report, the complaint to the judicial or accounting authority, or the public disclosure.

2.4 Public disclosure

The Whistleblowing Decree has introduced an additional reporting method known as public disclosure.

"Public disclosure" means "*making information on violations available to the public through the press, electronic means, or any other channels capable of reaching a large number of people*".

Such channels include social media, as well as communications to elected representatives, civil society organisations, trade unions, or business and professional associations.

Pursuant to Article 15, the whistleblower shall benefit from the protections provided by the Whistleblowing Decree only if, at the time of the public disclosure, at least one of the following conditions is met:

a) the whistleblower has previously made an internal and an external report, or directly an external report, and no response has been received within the prescribed time limits (for internal reporting: 3 months from the acknowledgment of receipt or, if no acknowledgment is issued, 3 months from the expiration of the 7-day period following submission; for external reporting: 3 months — or 6 months in duly justified cases — from the acknowledgment of receipt or, in its absence, from the expiration of the 7-day period following receipt of the report);

b) the whistleblower has reasonable grounds to believe, based on concrete circumstances, that the violation may represent an imminent or obvious threat to the public interest (e.g., an emergency or the risk of irreversible harm, including to the physical safety of one or more individuals), requiring immediate disclosure and broad dissemination to prevent harm;

c) the whistleblower has reasonable grounds to believe, based on concrete circumstances, that an external report may expose them to retaliation or may not lead to effective follow-up, due to the specific circumstances of the case (for example, fear that evidence may be concealed or destroyed, or that the recipient of the report may be colluding with or involved in the violation).

A person who engages in public disclosure must be distinguished from someone who serves merely as a source of information for journalists.

If the discloser voluntarily reveals their identity, the provisions on confidentiality will not apply, without prejudice to the other protective measures provided by the Decree.

However, where the disclosure is made using a pseudonym or nickname that does not allow identification of the author, ANAC will treat the disclosure as an anonymous report and will register it for record-keeping purposes. This is to ensure that, if the identity of the discloser becomes known at a

later stage, and the discloser declares to have suffered retaliation, the protections under the Decree may still apply.

2.5 Report to judicial and/or accounting authorities

The Whistleblowing Decree also grants protected individuals the right to report unlawful conduct, of which they have become aware within a public or private work context, directly to judicial authorities.

It is important to note that, if the whistleblower qualifies as a public official or as a person entrusted with a public service, the submission of a report through the internal or external channels provided by the Decree does not exempt them from the legal obligation to report criminally relevant facts or instances of damage to public finances to the competent judicial authority.

3. PROTECTION SYSTEM ACCORDING TO WHISTLEBLOWING DECREE

3.1 Individuals Entitled to Protection Measures

One of the main features of the entire framework established by the Whistleblowing Decree is the system of protection granted to those who report, publicly disclose, or denounce violations[2].

These protections will be examined in greater detail in the following paragraphs of this section of the Organisational Act.

However, it must be specified from the outset that the protection system established by the Legislator also extends to individuals other than the whistleblower, reporter, or person making the public disclosure. This includes people who, due to their role in the reporting, disclosure, or denunciation process and/or their particular relationship with the whistleblower or reporter, could be subject to retaliation, even if such retaliation is indirect.

Pursuant to Article 3, paragraph 5, the protection measures set out in Chapter III of the Decree also apply to the following individuals (for further details on the concrete identification of such individuals, please refer to the ANAC Guidelines of July 12th, 2023, and any subsequent amendments or additions):

- facilitators;
- people working in the same work environment as the whistleblower, the individual who has filed a complaint with the judicial or accounting authorities, or the individual who has made a

[2] individuals have been previously identified sub paragraph 1.3 "*Recipients*".

public disclosure, and who have a close emotional or family bond with them, up to the fourth degree of kinship;
- colleagues of the whistleblower, or of the individual who has filed a complaint with the judicial or accounting authorities or made a public disclosure, who work in the same work environment and have a regular and ongoing relationship with said person;
- entities owned by the whistleblower or by the person who has filed a complaint or made a public disclosure, or entities for which those people work, as well as entities operating in the same work environment as the aforementioned people.

3.2 Confidentiality protection

The protection system established by the Decree and implemented by the Company through the execution of all the requirements set forth therein ensures the confidentiality of the identity of the whistleblower (including any information, even indirectly inferable from attached documentation), the facilitator, the person involved, and any other individuals mentioned in the report (even when the report is submitted in a manner different from that prescribed or addressed to people other than the Reporting Manager).

Article 12 of the Decree establishes the obligation of confidentiality, stating that:

- paragraph 1 – reports may not be used beyond what is necessary to appropriately address them (principle of purpose limitation and data minimization – furthermore, under Article 13, para. 2, "*Personal data that are manifestly not useful for handling a specific report are not collected or, if accidentally collected, are immediately deleted*");
- paragraph 2 – the identity of the whistleblower and any other information from which it can be inferred, directly or indirectly, may not be disclosed without the express consent of the whistleblower, except to the Reporting Manager;
- Paragraph 3 – in criminal proceedings, the identity of the whistleblower is protected by secrecy in the manner and within the limits set forth in Article 329 of the Italian Code of Criminal Procedure[3];
- paragraph 4 – in proceedings before the Court of Auditors, the identity of the whistleblower may not be disclosed until the conclusion of the investigatory phase (after which it may be revealed by the auditing authority for the purpose of the proceeding itself);
- paragraph 5 – in disciplinary proceedings, the identity of the whistleblower may not be disclosed if the charge is based on findings that are separate and additional to the report, even if resulting from it. If the charge is based, in whole or in part, on the report and knowledge of the whistleblower's identity is essential for the defence of the accused, the report may only be used if the whistleblower gives express consent to the disclosure of their identity;
- paragraph 6 – the whistleblower is notified in writing of the reasons for the disclosure of confidential data, in the case provided for under paragraph 5 (disciplinary proceedings,

[3] This law establishes the obligation of confidentiality regarding the acts carried out during the preliminary investigations "*until the defendant is able to become aware of them and, in any case, no later than the conclusion of the preliminary investigations*."

second sentence), as well as in internal and external reporting procedures described in this chapter, when the disclosure of the whistleblower's identity and the information referred to in paragraph 2 is essential for the defence of the person involved;

- paragraph 7 – public and private sector entities, ANAC (National Anti-Corruption Authority), and the administrative authorities to which ANAC forwards external reports under their jurisdiction must protect the identity of the people involved and the people mentioned in the report until the conclusion of the related proceedings, ensuring the same safeguards provided for the whistleblower;
- paragraph 8 – reports are not subject to access under Articles 22 et seq. of Law no. 241 of 1990, nor under Articles 5 et seq. of Legislative Decree no. 33 of 2013;
- paragraph 9 – without prejudice to the provisions of paragraphs 1 to 8, in internal and external reporting procedures, the person involved may be heard or, upon request, must be heard, also through written proceedings involving the submission of written comments and documentation.

The confidentiality protection of people involved or mentioned in the report does not extend to cases of reports made to the Judicial Authority and the Court of Auditors. In these two cases, the Legislator limits confidentiality protection exclusively to the whistleblower.

Furthermore, regarding the possibility of public disclosure, confidentiality protection does not apply if the whistleblower has intentionally revealed their own identity through, for example, web platforms or social media. The same applies if the individual directly contacts a journalist.

However, if the person making the disclosure does not reveal their identity (e.g., by using a pseudonym or nickname on social media), such disclosures are treated as anonymous reports.

Within the 231 Organisational, Management and Control Model (MOGC 231), the Company has established a dedicated sanctioning system that provides for disciplinary penalties against those deemed responsible for violating the confidentiality obligation set forth in Article 12 of the Whistleblowing Decree.

3.3 Right to personal data protection

In order to guarantee the right to personal data protection for the whistleblower or complainant, the Legislator has established that the collection and management of reports, public disclosures, or complaints, including communications between competent Authorities, must comply with the applicable personal data protection regulations [in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and Legislative Decree no. 196 of 2003].

Any exchange and transmission of information involving the processing of personal data by EU institutions, bodies, or agencies must also comply with Regulation (EU) 2018/1725.

Personal data protection is ensured not only for the whistleblower or complainant but also for other individuals entitled to confidentiality protection, such as the facilitator, the person involved, and the person mentioned in the report, as they are “data subjects” affected by the data processing.

The following are the roles of the subjects who may process personal data under this regulation:

- Data Controller:
  - for the internal reporting channel: the Company;
  - for the external reporting channel: ANAC and/or other Authorities to which reports are forwarded;
- Joint Data Controllers:
  - public and/or private entities in cases where they share the same internal reporting channel;
- Data Processor:
  - provider of the Whistleblowing portal;
- Authorized Data Processor:
  - the Manager Responsible for the internal reporting channel and people expressly designated by the Data Controller or Joint Data Controllers to handle the reports.

Documentation concerning reports and related data is confidential.

Such documentation must be securely archived and managed in compliance with company procedures on information classification and processing, for the duration necessary to handle the report and, in any case, no longer than 5 years from the date of communication of the final outcome of the reporting procedure.

In the event of a violation of the above-mentioned regulations, the data subject may contact the Data Protection Authority.

3.4 Protection against retaliatory measures

Whistleblowing Decree prohibits the adoption of any retaliatory measures against the whistleblower and other expressly protected individuals.

Retaliation is defined as “*any behaviour, act, or omission, including attempted or threatened acts, carried out because of the report, the complaint to the judicial or auditing authority, or the public disclosure, which causes or may cause unjust harm, directly or indirectly, to the whistleblower or the person who filed the complaint* (including the entity itself).”

This is therefore a broad definition of retaliation, which can consist not only of acts or measures but also behaviors or omissions occurring in the workplace context that prejudice the protected individuals, including those that are only attempted or threatened.

An "*attempted retaliation*" refers, for example, to dismissal following a report, complaint, or public disclosure that the employer failed to execute due to a mere formal error in the dismissal procedure; "*threatened retaliation*" refers, for example, to the prospect of dismissal or change of duties expressed during a meeting between the person who made the report, complaint, or disclosure and their employer (in both cases, the protected individual must provide evidence from which the likelihood of the actual attempt or threat of retaliation can be inferred).

Article 17, paragraph 4, provides a (non-exhaustive and/or non-mandatory) list of possible retaliatory measures:

- dismissal, suspension, or equivalent measures;
- demotion or denial of promotion;
- change of duties, change of workplace, salary reduction, change of working hours;
- suspension of training or any restriction of access to training;
- reprimands or negative references;
- adoption of disciplinary measures or other sanctions, including monetary penalties;
- coercion, intimidation, harassment, or ostracism;
- discrimination or any other unfavourable treatment;
- failure to convert a fixed-term employment contract into a permanent contract where the worker had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or economic or financial prejudice, including loss of economic opportunities and income;
- inclusion in improper lists based on a formal or informal sectoral or industrial agreement, which may prevent the person from finding employment in the sector or industry in the future;
- early termination or cancellation of a goods or services supply contract;
- cancellation of a license or permit;
- request for psychiatric or medical examinations.

According to Article 19 of Legislative Decree no. 24 of 2023, any retaliatory measures may be reported to ANAC by the whistleblower and other subjects referred to in article 3, paragraph 5, through the digital platform provided by ANAC.

Article 16 establishes the conditions that must be met in order to benefit from the protection provided by the Whistleblowing Decree:

Paragraph 1, letter a): "*at the time of the report, the complaint to the judicial or auditing authority, or the public disclosure, the whistleblower or complainant had a reasonable belief that the information about the violations reported, publicly disclosed, or complained about was true and fell within the objective scope referred to in Article 1*". It is therefore necessary that the whistleblower, the person who made the complaint, or the person who made the public disclosure acted based on a reasonable conviction that the information on the reported, disclosed, or complained violations was truthful and within the scope of application of the Decree (mere suspicions or hearsay are not sufficient — this is the so-called relevance requirement). However, for the recognition of protections, it does not matter if the person reported, publicly disclosed, or complained without being certain of the actual occurrence of the reported facts or the identity of the perpetrator, or if some inaccuracies were reported due to a genuine error;

Paragraph 1, letter b): "*the report or public disclosure was made in accordance with the provisions of Chapter II*".

Both of these conditions must be met simultaneously, and there must be a close connection between the report/complaint/public disclosure and the unfavourable behaviour/act/omission suffered, directly or indirectly, for the latter to be considered "retaliation" and for the person who suffered it to benefit from the protection provided by the Decree (a causal link that must be verified by ANAC).

The same form of protection also applies to the so-called "facilitator" and other individuals assimilated to the whistleblower (already fully indicated in section 3.1 "*Subjects entitled to the protection measures indicated in this section of the Organisational Act*"), who—when the same conditions occur—may report any retaliatory measures adopted against them by ANAC due to their qualified connection with the whistleblower, complainant or public discloser.

If the conditions mentioned in article 16 are not met:

a) reports, public disclosures, and complaints will not be considered as falling within the scope of the Whistleblowing regulation, and therefore the protections provided will not be granted in favour of the whistleblower, the complainant, or the person who made the public disclosure;

b) likewise, protection is excluded for other individuals who, due to their role in the reporting/complaint process and/or their particular relationship with the whistleblower or complainant, have been subject to one of the acts, behaviours, or measures described above.

Furthermore, Article 16, paragraph 3, establishes that "*except as provided in Article 20, when the criminal liability of the whistleblower for the crimes of defamation or slander, or for the same crimes committed through complaints to the judicial or auditing authority, or their civil liability for the same reasons in cases of intent or gross negligence, is ascertained—even by a first-instance judgment—the protections under this chapter are not guaranteed and a disciplinary sanction is imposed on the whistleblower or complainant*".[4]

In conclusion, Article 16, paragraph 4, provides that "*the provision of this article also applies in cases of anonymous reports or complaints to the judicial or auditing authority or public disclosure, if the whistleblower is later identified and suffers retaliation, as well as in cases of reports submitted to the institutions, bodies, and competent agencies of the European Union, in accordance with the conditions set forth in Article 6*".

3.5 Support measures by Third sector Entities

To further strengthen the protection of the whistleblower, pursuant to Article 18 of the Decree, ANAC may enter into agreements with Third Sector entities so that they can provide support measures to the whistleblower.

Specifically, these entities, included in a special list published by ANAC on its institutional website, offer free assistance and advice on the reporting procedures, protection from retaliation as recognized by national and European Union regulations, the rights of the person involved, and the methods and conditions for accessing legal aid at the State's expense.

3.6 Limitations of liability for whistleblowers, complainants or public disclosers

Among the protections granted to whistleblowers, complainants, or those making public disclosures are limitations of liability concerning the disclosure and dissemination of certain categories of information.

These limitations apply only under specific conditions; in their absence, the person could incur criminal, civil, or administrative liability.

When these exonerating circumstances apply, the following offenses cannot be charged in relation to the disclosure of confidential information:

[4] However, ANAC has highlighted that the protections provided by the Decree may also be applied retroactively, should a conviction be subsequently overturned in favor of the whistleblower or complainant.

- disclosure and use of official secrets (Art. 326 of the Italian Criminal Code);
- disclosure of professional secrets (Art. 622 of the Italian Criminal Code);
- disclosure of scientific or industrial secrets (Art. 623 of the Italian Criminal Code);
- breach of the duty of loyalty and fidelity (Art. 2105 of the Italian Civil Code).

Nor can liability be imposed for:

- violations of copyright laws;
- breaches of data protection regulations;
- disclosure or dissemination of information concerning violations that may damage the reputation of the individuals involved.

These limitations of liability apply only when both of the following two conditions are met:

1) at the time of disclosure, there were reasonable grounds to believe that the information was necessary to reveal a violation. The person must reasonably believe—based on more than just suspicions or rumours—that the information was essential to uncover the wrongdoing, and not motivated by other purposes (e.g., gossip, revenge, opportunism, or sensationalism);
2) the report, public disclosure, or complaint was made in compliance with the conditions laid out in the Decree to qualify for protection against retaliation.

The entity or individual protected under the Decree shall not be held liable, including civil or administrative liability, for the acquisition of information concerning violations or access to such information, provided that such acquisition or access occurred lawfully and does not in itself constitute a criminal offense.

If the acquisition or access to the information or documents was achieved by committing a crime—such as unauthorized access or an act of cyber piracy—the exemption from liability does not apply. In such cases, criminal liability remains, along with any applicable civil, administrative, or disciplinary liability. It will be the responsibility of the judicial authority to assess the liability of the whistleblower or reporting entity, based on all relevant factual circumstances and the specific context of the case.

The legal justification applies only to acts, behaviours or omissions that are directly connected to the report, complaint or public disclosure and that are strictly necessary to uncover the violation.

To avoid liability, there must therefore be a close connection between the report, complaint or public disclosure and the conduct carried out or omitted.

Furthermore, the act, behaviour or omission must be strictly necessary—not excessive or superfluous—for exposing the violation.

If these conditions are not met, liability is not excluded, and it will be up to the judicial authority to assess the case based on all available factual information, considering the specific circumstances, including the necessity and proportionality of the act or omission in relation to the report, complaint or public disclosure.

3.7 Prohibition of waivers and settlements

Any waiver or settlement, whether full or partial, concerning the rights and protections provided by the Whistleblowing Decree, shall be considered null and void, unless made within the so-called “protected venues”, as defined under Article 2113, paragraph 4 of the Italian Civil Code. These venues include: proceedings before a judicial authority (Article 185 of the Code of Civil Procedure); proceedings before the conciliation commission established at the Territorial Labour Directorate (Article 410 of the Code of Civil Procedure); proceedings before certification bodies (Article 31, paragraph 13, Law no. 183/2010); proceedings before the conciliation commission set up in the trade union context (Article 412-ter of the Code of Civil Procedure); proceedings before unofficial arbitration and conciliation boards (Article 412-quater of the Code of Civil Procedure). Even more so, these rights and protections cannot be voluntarily waived by the protected person.

4. TRAINING AND INFORMATION ON THE CONTENT OF WHISTLEBLOWING DECREE

The Company considers training and information on the content of the Whistleblowing Decree to be a key element in correctly fulfilling the objectives set forth by the aforementioned legislation.

For this reason, the Company is committed to ensuring the continuous training and education of its employees on whistleblowing matters, with the aim of identifying reportable conduct and preventing inappropriate or unlawful behaviour.

Likewise, the Company undertakes to promote awareness and updates on whistleblowing regulations in its dealings with third parties (clients, suppliers, consultants, collaborators, and contractors), ensuring appropriate dissemination of the contents of this Organisational Act and, where required and/or appropriate, including specific contractual clauses governing the rights and obligations of each party.

5. UPDATE OF THIS ORGANISATIONAL ACT

This Organisational Act, the Whistleblowing Portal and all related documentation concerning the provisions currently set forth under Legislative Decree No. 24 of 2023 shall be periodically reviewed and updated to ensure continued alignment with the applicable legal framework.

6. ANNEXES

To this Organisational Act are attached the following annexes:

- annex 1a: conformity declaration of Whistleblowing portal issued by ISWEB S.p.A.;
- annex1b: declaration about security measures of Whistleblowing portal issued by ISWEB S.p.A.;
- annex 1: “ISWEB Cloud” certificate issued by ISWEB S.p.A.;
- annex 2: reporting form available on the Whistleblowing Portal provided by ISWEB S.p.A.

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00