WHISTLEBLOWING POLICY

PROCEDURE FOR IMPLEMENTATION AND MANAGEMENT OF REPORTS OF VIOLATIONS

Purpose	Define the process for managing any reports made by employees and collaborators to the Company, provide operational indications about scope, content, transmission methods, recipients, as well as forms of protection for people involved in the process.		
Scope:			
Edition:	1	**Date:**	03/12/2023
Revision:		**Date:**	
Review	Annually		
Reference number:			
Cross Reference Policies:	- Organisation, Management and Control Model pursuant to Legislative Decree 231/01 - Code of Ethics		
Further information:			
Authorised for release:			

CONTENTS

I - COMMON PROVISIONS

1. Premise

The Omnia Technologies Group has an interest in learning about any breaches that may occur within its organisation in order to effectively remedy them. To this end, it invites all those who are part of it to freely discuss any critical issues they may encounter in their work, certain that no one will retaliate against them for this.

However, where there is a desire to keep their identity confidential and/or a fear of retaliation by other members of the organisation, the Omnia Technologies Group allows reports to be made in a protected manner in the manner provided for in this procedure.

2. Purpose

The purpose of this document is to regulate the methods of making and managing reports of violations of national or European regulatory provisions that affect the public interest or the integrity of the Omnia Technologies Group Companies, as well as the protection measures for persons who make reports.

3. Recipients

This document applies to employees of Omnia Technologies Group Companies and, by virtue of a specific contractual clause, to all those who have self-employment, collaboration and professional consulting relationships with the Company, as well as to all persons who work for Omnia Technologies Group Companies.

This document also applies to the shareholders of the Omnia Technologies Group Companies and to all persons who perform, even de facto, administrative, management, control, supervisory or representative functions of the Company.

4. Adoption

The adoption and updating of this document is the responsibility of the Governing Body, after consulting the company trade union representatives or trade union organisations referred to in Article 51 of Legislative Decree 81/2015 regarding the internal reporting channel identified[1].

5. Communication and dissemination

This document is brought to the attention of the company staff at the time of adoption, in the event of updating and in any case at the time of selection and at the time of hiring.

At the time of first adoption, the company staff will be notified at the same time of whether or not each Company has exceeded the relevant dimensional threshold with respect to the identification of the violations subject to possible reporting and the reporting channels that can be activated (number of employees employed in the previous year). Any future changes will be communicated by 30 January of each year.

For third parties, this information can be found at the competent Chamber of Commerce, Industry, Crafts and Agriculture.

[1] Art. 4 paragraph 1 of Legislative Decree 24/2023.

This document is made easily accessible to company staff by posting it on the bulletin board and publishing it on the Company's Intranet website.

Clear information on the channel, procedures and conditions for making internal and external reports are published on the website of the Omnia Technologies Group Companies that are equipped with it.

The aforementioned obligations fulfill the information burden of the manager of the internal reporting channel[2].

6. Regulatory references

- Legislative Decree no. 231 of 8 June 2001,containing "Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant toArticle 11 of Law no. 300 of 29 September 2000";
- Directive (EU) of the European Parliament and of the Council of 23 October 2019, n. 1937, on the protection of persons reporting breaches of Union law;
- Legislative Decree no. 24 of 10 March 2023, "implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions for the protection of persons who report breaches of national regulatory provisions";
- Regulation (EU) No 679/2016 of the Parliament and of the Council of 27 April 2016on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Legislative Decree no. 196 of 30 June 2003,on the protection of personal data;
- UNI ISO 37002:2021 - *Whistleblowing management systems - Guidelines*;
- ANAC Guidelines "on the protection of persons reporting breaches of Union law and protection of persons reporting breaches of national regulatory provisions. Procedures for the presentation and management of external reports " approved by Resolution no. 311 of 12 July 2023;
- "New discipline "Whistleblowing" - Operational guide for private entities" of Confindustria of October 2023.

The regulatory references from which the respective provisions are taken are indicated in the footnotes of this document.

7. Definitions

For the purposes of this document, the following definitions apply:

a) "public disclosure": making information about violations public through the press or electronic means or in any case by means of dissemination capable of reaching a large number of people;
b) "manager": the person in charge of receiving and managing reports made through the internal reporting channel of Omnia Technologies Group Companies;
c) "confidential information": information covered by the obligation of secrecy, the protection of copyright or the protection of personal data;

[2] Art. 5 paragraph 1 lit. *and* Legislative Decree 24/2023.

d) "model": organisation, management and control model adopted by each Omnia Technologies Group Company pursuant to Legislative Decree 231/2001;
e) "connected persons":
   1) persons operating in the same working context who assist the whistleblower in the whistleblowing process (so-called facilitators);
   2) persons of the same working context linked to the whistleblower by a stable emotional bond or kinship within the fourth degree;
   3) colleagues who work in the same working context as the whistleblower and who have a habitual and current relationship with the same;
   4) bodies owned by the whistleblower, for which the whistleblower works or which operate in the same working context as the whistleblower (e.g.: companies belonging to the same business group);
f) "feedback": communication to the reporting person of information relating to the follow-up that is given or that is intended to be given to the report;
g) "retaliation": any behaviour, act or omission, even if only attempted or threatened, carried out by reason of the report, the complaint to the authority or public disclosure and which causes or may cause the reporting person or the person who made the complaint, directly or indirectly, unfair damage;
h) "whistleblower": the natural person who makes the report or public disclosure of information on violations acquired within their work context;
i) "reported": the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as the person in any case involved in the violation reported or publicly disclosed;
j) "report made in bad faith" or "report in bad faith": a report made by the whistleblower who, at the time of making the report, complaint or public disclosure, had not founded reason to believe that the information on the violation subject to reporting, complaint or disclosure was true;
k) "follow-up": the action taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigations and any measures taken.

8. Penalties

Violations of this procedure assume disciplinary relevance and will be sanctioned in compliance with the provisions of the internal disciplinary system. By way of example, the following constitutes a punishable violation:

a) making the report in bad faith;
b) the making of a report whose defamatory or slanderous nature has been ascertained by the Judicial Authority[3];
c) the disclosure of the identity of the whistleblower, connected persons and any other information from which their identity can be inferred;
d) any behaviour aimed at hindering reporting;
e) the attempt to identify the whistleblower[4];

[3] Art. 16 paragraph 3 of Legislative Decree 24/2023.
[4] UNI ISO 37002:2021, § 8.4.2.

f) the failure to manage the report for wilful misconduct or gross negligence, including the failure to remedy, by those who have the powers, the violations or retaliation reported;
g) the adoption of retaliatory behaviour.

Violations of this procedure by third parties, not employees of the entity, may be sanctioned by virtue of a specific contractual clause.

II - MAKING THE REPORT

9. Subject of the report

I may be subject to reporting[5], in the manner indicated in this document, violations or risks of violation[6] of national or European regulatory provisions that affect the public interest or the integrity of the Omnia Technologies Group Companies. In particular:

a) relevant unlawful conduct pursuant to Legislative Decree 231/2001;
b) violations of the Model, even if not constituting a crime.

If the company has employed, in the last year, more than 50 employees with permanent or fixed-term employment contracts, the following may also be reported:

c) offences falling within the scope of European and national legislation relating to the following sectors:
   - public procurement;
   - financial services, products and markets;
   - 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;
   - protection of privacy;
   - protection of personal data;
   - security of networks and information systems.

d) acts or omissions affecting the financial interests of the European Union or concerning the relevant internal market (e.g.: competition and state aid infringements);
e) acts or behaviours that defeat the object or purposes of the aforementioned regulatory provisions.

Disputes, claims or requests related to a personal interest of the whistleblower that relate exclusively to their employment relationships or their relationships with hierarchically superior figures are excluded from the scope of this document[7]. Such complaints may be communicated in the ordinary forms to the competent company functions.

[5] Articles 1-3 Legislative Decree 24/2023.
[6] UNI ISO 37002:2021, Introduction.
[7] Art. 1 paragraph 2 of Legislative Decree 24/2023.

In any case, unfounded reports made with intent or gross negligence are prohibited[8]. In such cases, the whistleblower will not be granted the protection measures provided for in this document and a sanction will be applied against them, in accordance with the provisions of the internal disciplinary system.

10. Subjects entitled to report

Reports may be made by those who have or have had working relationships with Omnia Technologies Group Companies[9]. In particular:

a) employees;
b) self-employed workers;
c) collaborators;
d) freelancers and consultants;
e) volunteers and trainees;
f) shareholders;
g) persons with administrative, management, control, supervisory or representative functions.

Reports can also be made before and regardless of the establishment of the employment relationship, where they relate to information acquired during the selection and/or probationary period[10].

11. Whistleblower Protection Measures

The whistleblower and related persons are entitled to the protections provided for in this document, provided that the report has been made in good faith and, in the event of external reporting or public disclosure, in the presence of the relevant conditions[11].

The reasons that lead the person to report are irrelevant for the purposes of their protection[12].

The protection measures also apply in cases of anonymous reporting, if the whistleblower was subsequently identified and retaliated against[13].

11.1. Confidentiality of the whistleblower's identity

The identity of the whistleblower is never revealed, without their express consent, to persons other than those competent to receive or follow up on the report[14], unless, as a result of the investigations carried out by the manager, the whistleblower appears to have made the report in bad faith or their responsibility emerges, also in conjunction with others, for the reported violation.

The same confidentiality is ensured for any other information from which the identity of the whistleblower can be deduced.

[8] Art. 16 paragraphs 1 letter *a* and 3 of Legislative Decree 24/2023.
[9] Art. 3 paragraphs 3 and 4 of Legislative Decree 24/2023.
[10] Art. 3 paragraph 4 letters *a* and *b*.
[11] Art. 16 paragraph 1 of Legislative Decree 24/2023.
[12] Art. 16 paragraph 2 of Legislative Decree 24/2023.
[13] Art. 16 paragraph 4 of Legislative Decree 24/2023.
[14] Art. 12 paragraph 2 of Legislative Decree 24/2023.

11.2. Prohibition of retaliation

The whistleblower cannot suffer any retaliation for having made the report[15].

The following constitute, by way of example, retaliation[16]:

a) dismissal, suspension or equivalent measures;
b) demotion or non-promotion;
c) the change of functions, the change of the workplace, the reduction of salary, the change of working hours;
d) the suspension of training or any restriction of access to it;
e) negative notes of merit or negative references;
f) the adoption of disciplinary measures or other sanctions, including financial penalties;
g) coercion, intimidation, harassment or ostracism;
h) discrimination or in any case unfavourable treatment;
i) failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had a legitimate expectation of such conversion;
l) the non-renewal or early termination of a fixed-term employment contract;
m) damage, including to the person's reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
n) placing on improper lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future;
o) the early conclusion or cancellation of the contract for the supply of goods or services;
p) the cancellation of a licence or permit;
q) the request to submit to psychiatric or medical investigations.

The prohibition of retaliation also applies to persons connected to the whistleblower[17].

11.3. Retaliation protection

Any retaliation suffered may be communicated to the ANAC, which informs the National Labour Inspectorate for the measures within its competence[18].

Retaliatory acts are void and the whistleblower and related persons are entitled to cessation of retaliatory conduct, compensation for damages and, in the event of dismissal, reinstatement in the workplace[19].

In the context of the related disputes established by the whistleblower, who claims to have suffered retaliation for making a report, the employer must prove that the act considered retaliatory is motivated by other legitimate reasons, unrelated to the report[20].

The waivers and transactions, in whole or in part, that have as their object the rights and protections provided for in this document are valid only if made in one of the locations provided

[15] Art. 17 paragraph 1 of Legislative Decree 24/2023.
[16] Art. 17 paragraph 4 of Legislative Decree 24/2023.
[17] Art. 17 paragraph 1 of Legislative Decree 24/2023.
[18] Art. 19 paragraph 1 of Legislative Decree 24/2023.
[19] Art. 19 paragraphs 3 and 4 of Legislative Decree 24/2023.
[20] Art. 17 paragraphs 2 and 3 of Legislative Decree 24/2023.

for by art. 2113 paragraph 4 of the Italian Civil Code (e.g. Territorial Labour Inspectorate; Certification Commission; Trade Union Office)[21].

11.4. Limitations of Liability

In the event that to make the report it is necessary to reveal confidential or offensive information of the reputation of the entity, the possible criminal, civil and administrative liability of the whistleblower and related persons is excluded[22], provided that the information is linked to the report and strictly necessary to reveal the violation[23].

In any case, the reports must relate to information acquired lawfully[24].

The making of the report does not, however, exempt the whistleblower from his/her possible responsibilities in relation to the reported violation[25].

11.5. Support measures

The list of Third Sector entities that provide support measures consisting of information, assistance and advice free of charge on reporting methods, on protection from retaliation, on the rights of the person involved in the reporting and on the methods and conditions of access to legal aid is established at the ANAC[26].

12. Internal reporting

Reports can be made through the *Integrity Line* application in the following ways[27]:

a) in written form, through the guided compilation of the fields within the application;
b) in oral form, through the recorded voice messaging system;
c) orally, at the request of the whistleblower, through a direct meeting with the manager of the whistleblowing channel[28] in a place suitable to guarantee confidentiality[29].

The *Integrity Line* application is accessible through the link to the following link https://omniatechnologiesgroup.integrityline.com/ from any device, which assigns the whistleblower a unique user profile to access to their reserved area and guides them in filling in some information fields for making a report as complete and detailed as possible or for requesting a meeting with the manager.

Regardless of the specific method chosen, the confidentiality of the identity of the whistleblower, the content of the report and the related documentation is in any case guaranteed.

13. Anonymous reporting[30]

Reports from which it is not possible to derive the identity of the whistleblower are considered anonymous.

[21] Art. 22 of Legislative Decree 24/2023.
[22] Art. 20 paragraphs 1 and 2 of Legislative Decree 24/2023.
[23] Art. 20 paragraph 4 of Legislative Decree 24/2023.
[24] Art. 20 paragraph 3 of Legislative Decree 24/2023.
[25] Court of Cassation, work sect., 31 March 2023, no. 9148 (ord.).
[26] Art. 18 of Legislative Decree 24/2023.
[27] Art. 4 paragraphs 1-3 of Legislative Decree 24/2023.
[28] Art. 4 paragraph 3 second sentence of Legislative Decree 24/2023.
[29] UNI ISO 37002:2021, § 8.2.
[30] LG ANAC, p. 33 s. and Operational Guide Confindustria, pp. 11 and 17.

Anonymous reports are not considered whistleblowing, therefore the manager will transmit them to the Governing Body, as received, for any consequent determinations, without prejudice to the recognition of the whistleblower's protections in the event of future identification.

14. External reporting and public disclosures

If the company has employed, in the last year, more than 50 employees with permanent or fixed-term employment contracts, the violation may be reported to ANAC[31], through the external channel activated by it, or publicly disclosed[32], when, alternatively:

a) the internal and/or external report, already made, has not been followed up;
b) the whistleblower has reasonable grounds to believe that, using the internal and/or external channel, the report would not be effectively followed up;
c) the whistleblower has a well-founded fear of retaliation;
d) the breach may constitute an imminent or obvious danger to the public interest.

III - MANAGEMENT OF THE REPORT

15. Person in charge of the management of the report

The receipt and management of the reports governed by this document are entrusted to the Supervisory Body of the Omnia Technologies Group Company concerned and to the Group Compliance Function[33] (in the event that the Company has an Organisation, Management and Control Model ex D.Lgs.231/01) and only to the Group Compliance Function in other cases.

The report submitted to a person incompetent to receive it is transmitted by the latter within 7 days of its receipt to the manager of the reporting channel, with simultaneous notification of the transmission to the whistleblower[34].

16. Receipt and acceptance of the report

In the event of a report made orally at the request of the whistleblower, the manager, with the consent of the whistleblower, documents the report by recording it on a device suitable for storage and listening or by means of a report, whose content must be submitted to the whistleblower for any changes and undersigning[35].

In the event of a report made through the *Integrity Line*application, by filling in the fields or by recording a voice message, the software records the report received and notifies the operator, who issues a notice of receipt to the reporting party within 7 days from the date of receipt[36]. The acknowledgement of receipt may include, but is not limited to[37]:

a) reassurance and request on the preferred methods for the continuation of the dialogue (e.g.: the report was made online but the reporter prefers to continue in person);

[31] Articles 6 and 7 of Legislative Decree 24/2023.
[32] Art. 15 of Legislative Decree 24/2023.
[33] Art. 4 paragraph 2 of Legislative Decree 24/2023.
[34] Art. 4 paragraph 6 of Legislative Decree 24/2023.
[35] Art. 14 paragraph 4 of Legislative Decree 24/2023.
[36] Art. 5 paragraph 1 lett. *a* legislative decree 24/2023.
[37] UNI ISO 37002:2021, § 8.1.

b) information on the subsequent phases of the reporting management process, its timing and possible results (e.g. what further feedback to expect and when);
c) information, including by reference to this procedure, on the measures taken to protect the reporting person, including measures to protect their identity, as well as on the responsibilities of loyal collaboration of the reporting person and of effective consideration and protection by the institution.

The manager diligently follows up on the report received[38] and provides feedback to the whistleblower within 3 months from the date of notice of receipt and in any case within 3 months and 7 days from receipt of the report[39].

Where investigations cannot be completed in a timely manner, for example because they are particularly complex, within the same period the manager shall update the whistleblower on the status of the report and inform them of the additional period of time necessary to complete them[40].

The deadlines for sending the notice of receipt and feedback are suspended at company closures and in any case from 1 August to 31 August and from 23 December to 7 January. If one of the terms referred to in this article expires during the period of weekday suspension of the terms, it will resume from the first working day following each period of suspension.

17. Preliminary assessment of the report

The manager carries out a preliminary examination of the report in order to verify whether it has as its object possible violations or retaliation falling within the objective and subjective scope of this procedure[41].

In the event that the whistleblower is not identified, the manager shall transmit the report to the Governing Body, as received, for any consequent determinations, keeping track of it and keeping the relevant documentation in accordance with the provisions of art. 26 of this document to allow its future traceability[42].

In the event that it considers that the report does not fall within the scope of this procedure, the manager shall notify the whistleblower, specifying the reasons and indicating the internal office that may be responsible for handling the reported problem. For the purpose of closing the report, the manager must prepare a special Report for the Governing Body and keeps an anonymised track of it in the Report Register.

In the event that it considers that the report falls within the scope of this procedure, the manager shall proceed to ascertain the reported violation as provided below.

18. Request for additional information

Where not already present in the report, the manager asks the whistleblower for the following information[43]:

[38] Article 5, paragraph 1, lett. *c* of Legislative Decree 24/2023.
[39] Art. 5 paragraph 1 lett. of *d* of Legislative Decree 24/2023.
[40] UNI ISO 37002:2021, § 8.2.
[41] UNI ISO 37002:2021, § 8.3.1, first point of the "Note" list.
[42] LG ANAC, p. 34 and Operational Guide Confindustria, p. 17.
[43] UNI ISO 37002:2021, § 8.2.

- Where did the breach take place?
- When did the breach occur (past, current, future, ongoing)?
- Who is involved in the breach?
- Have you reported it previously? If so, what, when and to whom? What action was taken?
- What is the impact for the organisation from your point of view?
- Is management involved or aware of the breach?
- Do you feel risks to yourself or others?
- Do you have documents or other evidence to support your report?
- Is there anyone else who is directly aware of the breach that we can contact?
- Has anyone tried to hide the breach or discourage you from sharing your concern? If so, who and how?

19. Prioritisation of reporting management (so-called triage)

In the presence of several reports to be handled at the same time, the manager assesses the urgency of intervention based on the probability of the breach and its potential impact on the institution, taking into account the following factors[44]:

- Can the violation become a criminal offence?
- Has the breach already happened, is it in progress, or is it about to happen?
- Is there an immediate need to interrupt or suspend business?
- Is there an immediate health and safety risk?
- Is there an immediate risk to human rights or the environment?
- Is there a need to secure and protect evidence before it is deleted or destroyed?
- Is there a risk to the functions, services and/or reputation of the institution?
- Can the report impact business continuity?
- What media impact can the report have?
- Is there any additional information available to support the report?
- What is the nature of the offence (type and frequency of the violation; role and seniority of the subjects involved in the reporting)?
- What is the probability that the breach will also be reported outside the institution?
- Has the breach been reported before?
- How did the whistleblower obtain the information: is the information "first-hand" or "by hearsay"?

20. Assessment of the reported violation

The manager proceeds to ascertain the reported violation by carrying out one or more of the following activities[45]:

a) involvement of competent company functions to support the assessment (e.g.: human resources; legal department; internal *audit*; compliance officer; health and safety; finance), unless this compromises the confidence of the whistleblower, the impartiality of the manager or the success of the investigation;
b) collection of documentary evidence in support of the report;
c) interviewing people able to report information useful for ascertaining the violation;

[44] UNI ISO 37002:2021, § 8.3.1.
[45] UNI ISO 37002:2021, § 8.3.1.

d) interview of the person reported, informing them in advance of the purpose of the meeting[46], which the manager must necessarily provide in the event of a request by the latter, also through the acquisition of written observations and documents[47].

The manager documents in writing the interviews carried out by means of a specific report, whose content must be submitted to the interviewee for any changes and signing.

During the assessment, the manager maintains discussions with the whistleblower and, if necessary, may request additions from the latter[48].

In any case, the manager protects the identity of the persons involved and mentioned in the report, until the conclusion of the assessment procedure[49].

21. Assessment and prevention of the risk of retaliation

The manager assesses the risk of retaliation for the whistleblower based on the following factors[50]:

- What is the likelihood that confidentiality will be maintained? For example: Is anyone else aware of the breach? Has the breach been reported to anyone else? Can the nature of the information reveal their identity? Are they the only ones with access to the information? Does the violation constitute a crime whose proof requires the identity of the whistleblower to be revealed?;
- Is the whistleblower worried about retaliation? Have retaliatory conduct already occurred or do you perceive an imminent risk of retaliation?;
- Is the whistleblower involved in the breach or did they suffer it?;
- Does the report cover different types of violations?;
- How did the whistleblower obtain the information about the breach?;
- What type of relationship exists between the whistleblower and the violation that is the subject of the report?;
- What kind of relationship is there between the whistleblower and the institution?

The level of protection and the related actions taken depend on the type and timing of the report and the potential consequences of the breach.

If the manager does not have the power to develop and implement strategies to prevent any damage to the whistleblower (eg: internal reorganisation of personnel), it notifies the whistleblower in order to allow the whistleblower to give their consent to the disclosure of their identity to those who, within the institution, have such power, without prejudice to the other protections provided for in this procedure in the event that retaliation is then effectively implemented.

22. Outcome of the checks carried out by the operator

The manager concludes the reporting management process by issuing a specific Report to the Governing Body, in which they report on the reporting management process and the outcome of the investigations carried out with particular reference to:

[46] UNI ISO 37002:2021, § 8.4.1.
[47] Art. 12 paragraph 9 of Legislative Decree 24/2023.
[48] Art. 5 paragraph 1 letter *b* of Legislative Decree 24/2023.
[49] Art. 12 paragraph 7 of Legislative Decree 24/2023.
[50] UNI ISO 37002:2021, § 8.3.2.

a) the non-existence of the reported violation or retaliation, specifying whether the report is considered to have been made in bad faith for the purposes of the possible application of the disciplinary sanction against the whistleblower;
b) the existence or risk of verification of the reported violation or retaliation, specifying the person held responsible and the elements collected.

The Report does not mention the identity of the whistleblower and other suitable information to identify them, except in cases of reporting made in bad faith or withholding responsibility of the whistleblower for the violation ascertained.

23. Actions resulting from the investigation of the violation or retaliation

The Management Body assesses the content of the Report and implements appropriate actions to the outcome of the assessments carried out by the manager. In particular:

a) in the event of incompleteness of the investigations carried out by the manager, it carries out further investigations, also through the competent company functions, a trusted defender or an external consultant;
b) in the event of an established violation or the risk of violation, it takes appropriate measures to prevent, interrupt or remedy the violation, as well as appropriate disciplinary measures against any person held responsible for the violation;
c) in case of withholding the existence of a concrete risk of retaliation, it takes appropriate measures to protect the whistleblower (eg: internal reorganisation of personnel);
d) in the event of ascertained retaliation, implemented or even threatened, against the whistleblower, it adopts appropriate measures to remedy the retaliation suffered[51] (e.g.: reinstatement of the whistleblower in the previous job position), as well as appropriate disciplinary measures against any person held responsible for the retaliation;
e) if the whistleblower is deemed to be in bad faith in making the report, it takes appropriate disciplinary measures against him/her.

The Management Body communicates the actions taken to the manager, so that it promptly responds to the whistleblower, and regularly monitors the effectiveness of the measures taken.

The reporting management process ends with the communication to the reporting party regarding the outcome of the investigations carried out and any actions taken as a result by the Governing Body.

24. Disciplinary procedure following the report

As part of the disciplinary procedure aimed at sanctioning the violation subject to reporting, the identity of the reporting person will not be revealed without their express consent, even if knowledge of their identity is essential for the defence of the reported person[52].

In order to allow them to express any possible consent, the manager communicates in writing to the whistleblower the reasons for the disclosure of confidential data[53].

[51] UNI ISO 37002:2021, § 8.4.3.
[52] Art. 12 paragraph 5 of Legislative Decree 24/2023.
[53] Art. 12 paragraph 6 of Legislative Decree 24/2023.

25. Processing of personal data

The activities of receiving and managing reports, including any consequent actions, involve the processing of personal data, which is implemented and organised by the Data Controller and the Co-owners of the processing, in compliance with current legislation and guaranteeing the data subjects, on the basis of what is applicable to such processing, the exercise of their rights referred to in Articles 15 to 22 of Reg. (EU) 2016/679 (see Annex).

EQS Group Srl based in Corso Vercelli, 40 - 20145 Milan (MI), as provider of the IT platform dedicated to the reception and management of reports, is Responsible for the processing of personal data on the basis of a specific appointment formalised in writing pursuant to art. 28 reg. (EU) 2016/679.

The Supervisory Body of the Omnia Technologies Group Companies and the Group Compliance Function, as managers of the reporting channel, are authorised to process personal data on the basis of a specific letter of appointment containing an indication of the confidentiality obligations that must be respected in the performance of the channel management function.

The information on the processing of personal data resulting from the receipt and management of reports is made available to allstakeholders on the *Integrity Line* application, which can be consulted at the following link https://omniatechnologiesgroup.integrityline.com/.

26. Preservation of documentation relating to reports

The reports are not used beyond what is necessary to give adequate follow-up to them[54]. In particular, personal data that are not useful for the processing of a specific report, where possible, are not collected and, if collected accidentally, are deleted immediately.

The manager keeps the reports and the related documentation for the time necessary to process them and in any case no later than 5 years from the date of communication of the final outcome of the reporting procedure[55].

In order to give evidence of the effective implementation of the system, the manager keeps an anonymised record of the reports received and managed in the specific Register of reports.

[54] Art. 12 paragraph 1 of Legislative Decree 24/2023.
[55] Art. 14 paragraph 1 of Legislative Decree 24/2023.

ANNEX

Information pursuant to the legislation on the protection of personal data (Articles 13-14) Whistleblowing

This document contains the information provided for in Articles 13 and 14 of EU Regulation 679/2016 (GDPR), in relation to the processing of personal data of data subjects who are involved, in various ways, in the reporting of relevant violations pursuant to the OMNIA TECHNOLOGIES Group Whistleblowing Procedure.

Dress up Privacy

The controller of the processing of personal data related to reports of relevant offences pursuant to D.Lgs.24/2023, relating to the company OMNIA DELLA TOFFOLA SPA is the same company.

Co-owners of the processing of personal data related to reports of relevant offences pursuant to D.Lgs.24/2023 relating to the other Group companies are the following companies:

COMPANY	REGISTERED OFFICE
Omnia Della Toffola SpA	Via Feltrina 72, 31040 Trevignano (TV) - Italy
Ape Officine Italia Srl	Via Ponte Perez 23 C/D, Zevio (VR) - Italy
Ave Tehcnologies Srl	Via Della Costituzione 127, 30038 Spinea (VE) - Italy
Gimar Srl	Via Casale 26, 15040 Occimano (AL) - Italy
Gruppo Bertolaso spa	Via Stazione 760, 37040 - Zimella (VR) - Italy
Progema Engineering Srl	Via Giovanni Verga 452, 46034 Pioppelle (MN) - Italy
Sirio Aliberti Srl	Region San Vito, 78 14042 Calamandrana (AT) - Italy
Z-Italia Srl	Via Brusche, 15, 46014 Castellucchio (MN) - Italy
F2 Srl	Via Giorgione, 25-26 - 31040 - Musano di Trevignano (TV) - Italy
Comas Srl	Via Toscana 22, 53036 Poggibonsi (SI) - Italy
TMCI Padovan Spa	Via Padovan 1, 31010 Mareno di Piave (TV) - Italy
TMCI Padovan Chemtech	Via Padovan 1, 31010 Mareno di Piave (TV) - Italy
SAP ITALIA SRL	Via S. Allende 1, 20077 Melegnano (MI) - Italy
Mar.Co srl	Strada Comunale San Vito 82/A, 14042 Calamandrana (AT) - Italy
Comes srl	Via dei Gelsi 17, Poggibonsi (SI) - Italy
Giuseppe Desirò srl	Viale Ludovico Ariosto 490 C/D, 50019 Sesto Fiorentino (FI) - Italy
Innotec srl	Via Enrico Fermi 13/C, 37135 Verona (VR) - Italy
Alfatre srl	Via Po 130, 20032 Cormano (MI) - Italy
Master Laser srl	Via Cesare Battisti 40, 20034 Cormano (MI) - Italy
Win&Tech srl	Via Pietro Nenni 8, 37024 Negrar di Valpolicella (VR) - Italia

The joint ownership relationship occurs, from time to time, exclusively between the parent company OMNIA OF TOFFOLA SPA and the individual subsidiary to which the report refers.

Without prejudice to the above, in particular, co-ownership refers to the processing of data carried out:

a) through the Admin role designated by OMNIA DELLA TOFFOLA S.P.A. configured in the back-end of the "Integrity Line" Portal/Software for the collection and management of reports, outsourced by OMNIA DELLA TOFFOLA S.P.A. in favour of the subsidiaries of the OMNIA TECHNOLOGIES Group, for the purposes of technical maintenance (e.g. 1st level help desk service) and management of the functional and security configurations available in the back-end of the Portal (e.g. modification of front-end texts, configuration of user roles – admin and

case manager - and of the privileges associated with them respectively, issuance of temporary passwords requested by users, etc.);

b) through the internal Case Manager appointed by OMNIA DELLA TOFFOLA SPA whose appointment has been contracted centrally by OMNIA DELLA TOFFOLA SPA also on behalf of the other subsidiaries that then outsource the related service, and/or

c) through any external Case Manager, whose professional mandate is contracted at any time by OMNIA DELLA TOFFOLA SPA also on behalf of all or some of the other subsidiaries, which will then outsource the related service;

d) through any other person authorised from time to time by OMNIA DELLA TOFFOLA S.P.A. and/or by the individual subsidiary of the Group to process the data for the purposes set out in this *Privacy Policy.*

The conditions and terms of the joint ownership relationship are governed by a *joint ownership agreement, contained in* the OMNIA TECHNOLOGIES Group *Whistleblowing Procedure* accessible through the Portal/software https://omniatechnologiesgroup.integrityline.com/, or available in the appropriate "whistleblowing" section of the following company websites https://www.dellatoffola.it and on the company's intranet website.

The Whistleblowing procedure will also be distributed to employees of the Group through the usual internal communication channels.

External data controllers are the third-party recipients of the data expressly indicated for this purpose in the chapter "Communication of personal data" below.

Personal data

The data we process may include:

- common personal data, including, for example, personal data (name, surname, date and place of birth, employment relationship with our Company or with the third-party organisation to which the whistleblower belongs), contact data (landline and/or mobile telephone number, postal/email address), job role/task, behaviours or other factual or legal circumstances referable to the whistleblower as well as similar types of data referable to natural third parties (e.g. subjects held responsible for the acts or omissions reported, witnesses, etc.);
- "special" personal data pursuant to art. 9 of the GDPR, including, for example, information relating to health conditions, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership;
- sporadically, "judicial" personal data referred to in art. 10 of the GDPR, relating to crimes and criminal convictions, or to related security measures (as a rule following the conclusion of the investigation following the report when criminal proceedings are initiated against natural persons; in addition, the data may include data and omissions punishable by a court or an administrative authority). These data must be processed only in cases of absolute necessity, are documented in writing and retained only to the extent strictly necessary after the decision on the offence has become final in a proceeding in which they have been processed; storage takes place, if possible, without reprocessing.

Personal data may be acquired by the Company as contained in the report or in the deeds and documents attached to these annexes, or through persons who are consulted by us during the related investigations (e.g. witnesses or other persons informed of the facts, managers of the report).

The persons to whom the personal data processed refer are, among other things, i) persons aware of the reported facts, or who in any case are requested to provide information in the face of a report ii) "subjects involved" (i.e. blamed for the violation subject to the report), iii) "protected subjects" (i.e. who enjoy the mandatory protections provided by the whistleblowing legislation in the face of a report), iv) Case Manager natural persons, v) other persons who for various reasons can be made aware of the existence and follow-up of the report.

Whistleblowers who process personal data of which they are aware beyond what is necessary to follow up on the report, assume the role of Data Controllers pursuant to Article 4 no. 7 of the GDPR.

Communication of personal data

The Data Controller, in compliance with the protection of the confidentiality of the identity of the whistleblower, may share the data, in accordance with the principle of strict necessity, proportionality and minimisation, with:

a) Other internal functions of the Data Controller, duly authorised, that the Case Managers deem appropriate to involve in the follow-up actions of a report;

b) Case Managers, that is, any third parties designated by the receiving company to admit and/or examine the report on the merits and/or to adopt the consequent actions, including feedback to the whistleblower;

c) Third parties expressly designated as External Data Processors (e.g. for purposes of hosting, maintenance or technical management of the datacenter, the online platform used to execute and manage the report and the related database);

d) Competent external authorities (e.g. judicial or administrative authorities, police bodies, finance guards, ANAC – National Anti-Corruption Authority, etc.) only in the context of a criminal, administrative or civil investigation or trial. In this case, the communication is subject to the guarantees provided for by the applicable regulations. In particular, the whistleblower is informed before his/her identity is revealed, unless such information would jeopardise the investigation or judicial proceedings. When the Competent Authority informs the whistleblower, it sends the whistleblower a written statement explaining the reasons for the disclosure of the confidential data in question:

e) Law firms and/or legal consultants, corporate compliance consultants and/or other subjects necessarily involved in the process of activating the reporting or management system of the report, in the adoption of corrective measures consequent thereto, or for the performance of any applicable sanctioning or criminal proceedings (e.g. lawyers and law firms, experts, technical consultants, investigative agencies, other subjects to whom the investigation and/or decision of the reports are delegated).

f) Any autonomous third party entitled to receive and process the data according to the Whistleblowing Procedure or the law.

In any case, the processing of data by other subjects will be lawful, including communication to third parties, when necessary for the adoption of corrective measures by the Companies or the activation of sanctioning or criminal proceedings.

Data security and confidentiality

We maintain adequate technical and organisational measures to guarantee data protection and confidentiality, without prejudice to the provisions of art. 12 of Legislative Decree no. 24/2023 - with particular reference to the identity of the whistleblower, the persons involved and/or in any case mentioned in the reports, their content and related documentation. The internet

communication channel used by the platform is encrypted using advanced protocols. The data will be stored in an encrypted format at an ISO 27001 certified datacenter located in Germany.

The data are processed analogically and electronically.

The right not to see their identity revealed to the persons to whom the reported facts refer (without prejudice to the limited exceptions deriving from any wilful misconduct or gross negligence of the whistleblower) or to third parties belongs not only to the whistleblower but also to those who have made a possible public disclosure of a violation provided for by the Data Controller's Procedure.

Dissemination. Data transfer outside the EEA.

The data will not be disclosed, except in the cases specifically provided for by national or European Union law. Data may be transferred to data centers in Germany. The data will not be transferred outside the EEA.

Purpose and legal basis

The data will be processed for the following purposes: i) assessing the admissibility and reasonableness of the report of offences communicated by you, ii) applying the protection and support measures of the subjects protected by the legislation on whistleblowing, iii) following up on the report and, if possible, responding to the results of a report, iv) applying any disciplinary measures or other sanctions against those who report with intent or gross negligence, or against any subjects involved to whom the reported violation is attributable, v) defending or ascertaining our rights in the context of judicial, administrative or extrajudicial proceedings and in the context of civil, administrative or criminal disputes arising in relation to the report made, vi) fulfilling any obligation provided for by law, regulation or other applicable legislation.

Taking into account the relevant legislation, the processing of data is based on the legal obligation to which the Company is subject as Data Controller (Article 6, paragraph 1, lett. c) of the GDPR) for the purposes of compliance with the requirements of Legislative Decree 24/2023 (as well as, in the case of companies with a Management, Organization and Control Model 231, also pursuant to Legislative Decree 231/2021 et seq.), and, with regard to any particular data voluntarily reported by the Whistleblower, the enabling condition is to be found in the reasons of relevant public interest on the basis of Union and Member State law in relation to the reason for which the whistleblowing legislation was established (Article 9, par. 2, letter g) of the GDPR and art. 2 sexies par. 1 of Legislative Decree 196/03), as well as, in relation to particular data, in the fulfilment of obligations and on the exercise of specific rights of the Data Controller and the Data Subject in the field of labour law (art. 9, par. 2, lett. b), GDPR).

Further clarification on the legal basis

The prior consent of the Whistleblower will be required from time to time (art. 6 par. 1 letter a) of the GDPR) as required by the Whistleblowing Decree, in particular:

- when the Report is made through a recorded voice messaging system (as provided for in the Procedure), in order to allow, by the personnel in charge, the relative documentation by recording on a device suitable for storage and listening or by full transcription. In the event of a transcript, the reporting person may verify, correct or confirm the content of the transcript by signing it;
- when, at the request of the reporting person, the report is made orally during a meeting with the staff, so with the prior consent of the reporting person, the report is documented by the staff by recording on a device suitable for storage and listening or by minutes. In the case of minutes, the reporting person can verify, correct and confirm the minutes of the meeting by signing them.

The legal basis of the processing for the purposes under i), ii) and iii) (in relation to the purposes of implementing response measures to the results of a report, strictly necessary to remove the consequences of the reported Breach) is the need to comply with the obligations provided for by the Data Controller by law, regulation or other legislation.

In relation to the purposes of implementing measures to respond to the results of a report, possibly different from those strictly necessary to remove the consequences of the reported Breach, the legal basis is the legitimate interest of the Data Controller to improve the organisation's structure.

In relation to disciplinary or sanctioning purposes, the legal basis is the legitimate interest of the Data Controller to pursue in disciplinary or sanctioning proceedings any non-compliance with the Data Controller's Whistleblowing Procedure and/or, more generally, with the legislation relating to whistleblowing. In relation to the purposes of defending or ascertaining our rights in the context of judicial, administrative or extrajudicial proceedings and in the context of civil, administrative or criminal disputes arising in connection with the report made, the legal basis is the legitimate interest of the Data Controller to exercise the defense of its rights.

Duration of storage

Personal data that appears not reasonably relevant and useful to the processing of a specific Report is not collected or, if received or collected accidentally, must be promptly deleted by the Report Managers responsible for the Breach.

Likewise, any personal data reported and referring to behaviours not included in the scope of the law and/or the Whistleblowing Procedure of the Data Controller will be deleted.

If the information received contains particular personal data pursuant to art. 9 of the GDPR, it will be deleted immediately, without being recorded and processed. If it is established that the information provided or part of it is not true, it must be immediately deleted as soon as this circumstance emerges, unless the lack of trithfulness may constitute an offence, in which case the information will be kept for the time necessary during the legal proceedings.

The reporting data and the related documentation will be kept for the time necessary to process the report and in any case no later than 5 (five) years (in Italy) from the date of communication of the final outcome of the reporting procedure (in compliance with the obligations of confidentiality of information as well as limitation of storage, provided for by the applicable regulations). After this period, the reports will be deleted from the system, or stored in an anonymised form, without prejudice to any need for storage for all the further time necessary for the completion of an administrative or judicial procedure already initiated or for investigative proceedings pursuant to the Code of Criminal Procedure.

Rights of data subjects

The data subject, in the person of the Whistleblower or the Facilitator, has the right to access at any time the data concerning him or her and to exercise the rights provided for in Articles 15 to 22 of the GDPR, as applicable (right of access to personal data, right to rectify them, right to obtain cancellation or so-called right to be forgotten, right to restriction of processing, right to portability of personal data or right to object to processing), by sending an email to: whistleblowing@omniatechnologiesgroup.com. The aforementioned rights cannot be exercised by the person involved or by the person mentioned in the report, for the time and to the extent that this constitutes a necessary and proportionate measure, pursuant to art. 2 undecies of the Privacy Code since the exercise of these rights could result in an effective and concrete prejudice to the protection of the confidentiality of the identity of the reporting person.

December 2023

Omnia Della Toffola SpA