WHISTLEBLOWING POLICY		
CREATED	ADACTA ASSOCIATED STUDIO	
CONTROLLED	GIULIA CHIARA PAOLONI	
APPROVED	FRANCESCO SCARPARI	
Protocol **contact person** *Responsible for storage, updating, dissemination and enforcement*	GIULIA CHIARA PAOLONI	
VERSION	1.0	
DATA	14.07.2023	

Index

1. PURPOSE

This procedure governs[1] the way in which the companies, as legal entities in the private sector, fulfil their obligation to establish a system for handling Reports (channels, procedures, resources) and to guarantee the Whistleblowers the Safeguards provided for by law and by the procedure itself.

The procedure is intended to facilitate the correct implementation of Community law (legal certainty) and thus ensure the 'well-being' of companies.
The objective is the 'transparency' of private action, which is the way to a truly virtuous company. Companies also handle Reports to avoid incurring detrimental effects related to Violations (e.g. negative publicity on the market).

2. DEFINITIONS AND SCOPE

2.1. Definitions

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

ANAC - National Anti-Corruption Authority (or **Competent Authority**)	*Italian independent administrative authority designated to (i) receive External Reports and (ii) carry out the functions provided for by the Directive, including feedback to the Whistleblower, in particular with regard to the follow-up given to Reports, in the cases provided for by the Whistleblowing Decree.*
Sectoral Acts	*normative acts identified in **Appendix A** of this procedure*
Reporting Channels	*channels for making the Report, made available to the Whistleblower, respectively, by the Companies, in the case of Internal Reporting, or by ANAC, in the case of External Reporting; These Internal Reporting Channels in turn are defined as Internal or External depending on whether they are managed directly by the companies or respectively by third parties authorised by them*
Work context	*work or professional activities, present or past, carried out within the framework of legal relations, through which, irrespective of the nature of such activities, a person acquires information on Violations and in the context of which he/she could risk being retaliated against in case of a Report or Public Disclosure or a complaint to the Judicial Authority*
Whistleblowing Decree	*Legislative Decree 24/2023 transposing the Whistleblowing Directive in Italy*
Public Disclosure	*making information on Infringements publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people (e.g. radio, television, blogs, Internet, automated e-mail campaigns)*

[1] In compliance with i) art. 6 paragraph 2 of Legislative Decree 231/01 as amended by Law no. 179 of 30 November 2017 on "Provisions for the protection of the authors of reports of offences or irregularities of which they have become aware in the context of a public or private employment relationship", ii) Legislative Decree 24/2023 implementing EU Directive 1937/2019 (the "Directive"), as well as iii) by the best practices applicable in this field (ISO 37002).

Whistleblowing Directive	*EU Directive 2019/1937 on the protection of persons who report breaches of Union law*
Third Sector Entities	*Entities that have entered into agreements with ANAC to provide Support Measures*
Facilitator	*a natural person who assists a Whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential*
Report Manager(s) (or 'Case Manager' in the Portal/Software)	*person(s) designated by the Companies to receive the Report and carry out the further related activities provided for in Chapter 3.5 of this procedure*
GDPR	*EU Data Protection Regulation 679/2016*
Group	*The corporate group to which the Company(ies) belongs*
HSchG	*HinweisgeberInnenschutzgesetz (federal law on protection in case of information on violations of law in certain sectors, transposing the Whistleblowing Directive in Austria, dated 01.02.2023 and in force from 25.02.2023)*
Information on Violations	*information, including well-founded suspicions, concerning:* *i) Violations committed or which, on the basis of concrete evidence, could be committed in the organisation with which the Whistleblower or the person making the complaint to the judicial or accounting authority has a legal relationship; and* *(ii) elements concerning any conduct aimed at concealing such breaches*
Protection measures	*measures provided for in paragraph 2 of* ***Appendix B*** *of this procedure*
Support Measures	*measures provided for in paragraph 6 of* ***Appendix B*** *of this procedure*
Person involved (Reported)	*natural or legal person mentioned in the internal or external Report or in the Public Disclosure as a person to whom the Breach is attributed or as a person otherwise implicated in the reported or publicly disclosed Breach*
Portal/Software	*the third-party cloud portal, accessible on the Internet at www.salvagnini.integrityline.com, which can be used by the reporter to make an Internal Report*
Procedures	*the set of directives, instructions, protocols and written procedures envisaged and implemented by the Company in order to prevent Breaches, and/or to reduce their consequences or recurrence*
Independent External Professional	*The external party (natural or legal person), autonomous and trained, other than the Supervisory Board 231 and the Data Protection Officer (if any), designated by one or more Companies as the Case Manager.*

Legal relationship	*legal relationship between the reporter and the organisation in which a breach has been committed or may be committed;* *the legal relationship may be direct or indirect (i.e. through a third party having a direct legal relationship with the Company(ies))*
Feedback	*communication to the Whistleblower of information on the Follow-up that is given or that is intended to be given to the Report*
Retaliation	*any conduct, act or omission, even if only attempted or threatened, committed by reason of the Report or of the complaint to the judicial authority or of the Public Disclosure and which causes or is likely to cause, directly or indirectly, unjust damage to the person making the Report or the complaint*
Administrative sanctions	*administrative pecuniary sanctions to be imposed by ANAC in respect of the non-compliance provided for therein*
Disciplinary sanctions	*disciplinary sanctions applicable by the Companies in the event of non-compliance with the provisions of this procedure*
Whistleblower	*a natural person, as referred to in Chapter 2.2.3, who makes a Report or Public Disclosure of Violation Information acquired in the course of his/her work context*
External Report	*written or oral communication of Breach Information by the Complainant submitted through the Reporting Channel activated by ANAC*
Internal Report	*written or oral communication of Breach Information, submitted through the Reporting Channels made available by the Companies*
Follow-up	*action taken by the Case Manager to assess the existence of the reported facts, the outcome of the investigation and any measures taken*
Company	*Any of the companies listed in Chapter 2.2.1 below*
Private Sector Subjects	*entities, other than those falling under the definition of Public Sector Entities*
Public Sector Entities	*public administrations referred to in Article 1(2) of Legislative Decree 165/2001,* *public economic entities,* *bodies governed by public law referred to in Article 3(1)(d) of Legislative Decree 50/2016,* *public service concessionaires,* *publicly controlled companies referred to in Article 2(1)(m) of Legislative Decree 175/2016, even if they are listed,* *in-house companies referred to in Art. 2(1)(o) of Legislative Decree 175/2016, even if listed*
External Subjects	*Whistleblower other than Internal Stakeholders*
Internal Subjects	*whistleblowers defined as internal in the table in Section 2.2.3 of this procedure*
Protected Subjects	*The persons envisaged in **para. 1 of Appendix B** to this Procedure, who are eligible for the Protections*

Safeguards	*the set of Protection and Support Measures provided for in the Whistleblowing Decree*
Breaches/violations of Sectoral Acts	*conduct, acts or omissions that harm the public interest or the integrity of the Companies and that consist of offences falling within the scope of the Sectorial Acts identified in* ***Appendix A****, which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly also different from the Company(ies), e.g. a supplier of the same or a contact person of an auditing firm of the same) with which the Whistleblower has a legal relationship,* *including any conduct aimed at concealing such violations,* *regardless of the fact that:* *- the employment relationship with the companies has ended in the meantime (so-called former employee), or that* *- the facts were learnt during the selection process (e.g. candidate) or in other pre-contractual negotiations with the companies,* *regardless of whether, under national law, Whistleblowing violations are administrative, criminal or purely civil violations (e.g. risk of damages).*

2.2. Subjective scope

2.2.1. This procedure applies to the following companies:

- ✓ **SALVAGNINI ITALIA S.P.A.**, with registered office at Via Ingegnere Guido Salvagnini, 51, 36040 Sarego (VI) - Italy (the '**Parent Company**')
- ✓ **SALVAGNINI INDUSTRIALE S.P.A.**, with registered office in Via Arcella, 122/I, 83030 Montefredane (AV) - Italy,
- ✓ **SALVAGNINI MASCHINENBAU GmbH**, headquartered at Dr. Guido Salvagnini-Straße 1, 4482 Ennsdorf - Austria

(the '**Companies**').

From time to time, it will be specified in this Procedure whether different and/or additional rules to those applicable in Italy apply in connection with Reports concerning SALVAGNINI MASCHINENBAU GmbH.

2.2.2. In relation to the aforementioned companies, this procedure applies:

- to Whistleblowers who make i) Internal and/or External Reports or ii) Public Disclosures or iii) Complaints to the Judicial Authorities, in relation only to the Sectorial Violations set out in ***Appendix A***,
- to the other Protected Subjects;
- other stakeholders who are involved in various ways in the Follow-up to Reports.

2.2.3. Whistlebowers may belong to the following categories:

ID	Subject category	Subject nature
A	Company **employees**, including occasional workers	Internal Subject

B	Paid and unpaid volunteers and **trainees** working for the companies	Internal Subject
C	**Self-employed workers, including** self-employed relationships that have special rules pursuant to Article 2222 of the Civil Code (work contracts) (including **freelancers and consultants** working for companies) as well as **Holders of a collaboration relationship as referred to in Article 409 of the Code of Civil Procedure, who** perform their work for the Companies, by which is meant 1) those of private employment, even if not inherent in the exercise of an undertaking; (2) agency, commercial representation relationships; and 3) other collaborative relationships resulting in the provision of continuous and coordinated work, mainly of a personal nature, even if not of a subordinate nature	External Subject
D	**Employees and collaborators**, who work **for third parties Public or private sector entities that provide goods or services or carry out works in favour of the companies**	External Subject
E	**Shareholders**	External Subject
F	**Members of the administrative and/or management** or representative **bodies of** the Companies, including non-executive members (e.g. directors without or with delegated powers), even when such functions are exercised on a de facto basis	Internal Subject
G	**Members of the control or supervisory body of** the companies (e.g. Board of statutory auditors, Auditors or Auditing Companies, Supervisory Board 231, DPO - Data Protection Officer)	Board of statutory auditors - ODV 231: Internal Subject Auditor or contact person of Auditing company - DPO: External Subject

2.3. Objective scope

Whistleblowers are obliged to communicate well-substantiated Infringement Information based on precise (adequately detailed) and concordant facts, and not facts of a general, confusing and/or blatantly defamatory or slanderous content.

Complaints**, claims or demands linked to a personal interest of the whistle-blower** or the person lodging a complaint with the judicial authority **that relate exclusively to his or her individual employment relationships, or inherent to his or her employment relationships with hierarchically superior figures,** will not be taken into account.

Reports **may also be anonymous**, i.e. they may not show the identity of the reporter or allow the identity of the reporter to be reconstructed or found. They will be examined, provided they comply with the above requirements.

Stand still:
(i) the application of the provisions on (a) the exercise of the right of workers to consult their representatives or trade unions, (b) protection against unlawful conduct or acts carried out as a result of such consultations, (c) the autonomy of the social partners and their right to enter into collective agreements, and (d) the suppression of anti-union conduct, and
(ii) the application of the provisions of criminal procedure (therefore, the Whistleblower will always be entitled, in the event that he/she has information about a criminal act, to lodge a complaint with the competent criminal authority).

3. REGULATION OF ACTIVITIES

3.1. Generalities

The Report is:

a) **obligatory**, on the part of the **Internal Parties** (NB. by virtue of the **general duties of loyalty, diligence and good faith** connected with the legal relationship with the Companies, to be understood as expressly reaffirmed herein)

b) **compulsory**, by **External Parties** who are **contractually obliged to** the Companies to report;

c) optional, by **External Parties** to the Companies that are not contractually obliged towards the Companies to report.

3.2. Subject of the Report

In order to facilitate and allow the due verifications and preliminary investigation activities by the Companies, also in order to ascertain the merits of the Report, the Whistleblower is suggested to provide at least the **following** useful **elements:**

- the **identity** of the reporter (name, surname, tax code, position or function held), unless the reporter decides not to proceed with an anonymous Report;
- a description of the **reasons** related to the work performed that made the reported facts known;
- a clear and complete **description of the facts that are** the subject of the Report;
- the **circumstances of time and place** in which the acts were committed, if known;
- the **particulars** of the person to whom the violation is attributed or elements useful for identifying him/her, if known;
- an indication of any **other persons who may report** on the facts that are the subject of the Report;
- an indication of any **documents that** may confirm the facts that are the subject of the Report;
- any other **information** that may provide useful feedback on the existence of the reported facts.

3.3. Types of Reports

A **Report** is defined:

a) **Internal**, if directed to the Companies[2] ; in which case it may be through one or more of the **Reporting Channels** (in turn distinguished as **internal or external**, depending on whether they are managed by the Companies or by third parties),

b) **External**, if executed **to the competent authority**,

c) **Public disclosure** if carried out in the presence of the specific prerequisites laid down by the Whistleblowing Decree for the latter.

3.3.1. Internal Signalling Channels

Internal Reporting Channels must be activated **after a mandatory hearing of trade union representatives or organisations.**

Internal Reporting Channels are distinguished into Internal and External, depending on whether they are managed directly by the Companies or, respectively, by third parties authorised by them.

The following Internal Reporting **Channels** may be used by the Whistleblower.

✓ INFORMATORS:

- **Portal/Software**[3] , accessible at **https://salvagnini.integrityline.com**,

✓ ORALS:

- **Voice recording** (to a registered voicemail/voicemail box) possible in the Portal/Software.
  The Case Managers are obliged to document the oral Report by means of a **detailed written account of** the conversation.
- *(at the request of the Whistleblower)* **Direct personal meeting** with one or more Case Managers, including via remote videoconference session if necessary.

  The Case Manager shall in such a case ensure, **with the necessary consent of** the reporter, that
  a) the meeting takes place **within a reasonable period of time** from the date of receipt of the aforementioned request (in Austria: maximum 14 working days), and

  are obliged to **document** the meeting through:
  b) **audio recording of the conversation on a durable audio medium** allowing access to the Information; or
  c) **detailed** and complete **record of the** meeting and conversation held.
  d) **transcription/upload and storage of the aforementioned minutes on the Portal/Software**.

[2] The Whistleblower must first check whether it is possible to communicate the Breach Information by means of an Internal Report, i.e. by using one of the Reporting Channels (internal or external) managed by the Company.
The use of an External Report or Public Disclosure is permitted only in the cases strictly provided for.

[3] Instructions for the use of the Portal/Software by the reporter can be found on the first online page of the Portal/Software.

If the Whistleblower has disclosed its identity, or, in the case of an anonymous Report, this is also possible without disclosing identity, the Case Managers must give the Whistleblower the opportunity to **verify, rectify and approve** the Report by its own signature.

Withdrawal of consent by the Whistleblower shall not affect the lawfulness of the processing and communication carried out on a voluntary basis until the withdrawal.

The Case Managers then manage the Follow-up of the Report via the Portal/Software.

NB: If a person other than the competent Case Managers receives a Report, he/she must forward it to the competent Case Managers, within 7 (seven) days from its receipt, complete with any supporting documentation received, not retaining any copy of it and refraining from taking any independent initiative for analysis and/or investigation.

Failure or delay in communicating the Report to the competent Case Managers by the first non-competent recipient constitutes a breach of this procedure, punishable as provided for in Section 9 below.

If the content of a Report comes to the knowledge of persons other than the Case Managers, in particular because a Report has not reached the relevant Case Managers directly, it is forbidden to disclose the content of the Report or the identity of the Whistleblower, except by forwarding the Report to the relevant Case Managers.

3.3.2. External Reporting and Public Disclosure

3.3.2.1. External Signalling

The Whistleblower may only issue an External Report if one of the following **conditions** is met when it is submitted:

a) there is no compulsory activation of any Internal Reporting Channel within its work context, or

b) the Internal Reporting Channel, although theoretically envisaged as mandatory for companies, is in fact **not active or, even if activated, does not comply** with regulatory requirements;

c) the Internal Report already made by the Whistleblower **had no Follow-up**[4] ;

d) the Whistleblower has **reasonable grounds to believe** that, if he or she made an Internal Report, it would not be effectively followed up or the Report might lead to the **risk of retaliation**;

e) the Complainant has grounds to believe that the breach may constitute an **imminent or obvious danger to the public interest**.

In Italy

External Reporting is made to ANAC:

- in **writing** through the Reporting Channel activated by ANAC

[4] In the event that the Report is closed with a negative final decision, a Report to the ANAC is therefore not allowed.

(for more information on contact details and instructions on the use of the External Reporting Channel, the confidentiality regime applicable to External Reports and the process for handling External Reports see https://www.anticorruzione.it/-/whistleblowing), or

- **orally** through (i) **telephone lines** or (ii) **voice messaging systems** or, (iii) at the request of the Whistleblower, through a **face-to-face meeting** set within a reasonable time.

In Austria

External Reporting of Violations for the different types of corruption set out in ***Appendix A*** can be made to the "Single Point of Contact (SPOC) for Corruption and Abuse of Authority" set up at the Federal Office for Prevention and Combating against corruption (**BAK - Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung**, website: http://www.bak.gv.at/), through:

• ordinary mail to: BAK - Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung - Herrengasse 7 - 1010 Vienna - Austria

• telephone +43 1 53 126-906800

• fax +43 1 53 126-108583

• email BMI-III-BAK-SPOC@bak.gv.at.

Although the Whistleblower always has the option of remaining anonymous, it is advisable to provide at least one contact address, because in many cases more detailed information is needed to carry out the investigation. In many cases, based on the rules governing criminal and police investigations, it may be essential to disclose the source of the report, even if made anonymously.

BAK is not competent to the extent that other federal authorities or agencies are responsible for Information on Violations of the Law.
A list of these other federal authorities and bodies can be found in the Federal Act on the Procedure and Protection of Whistleblowers (HScgG), Section 3, Article 'External Bodies for the Receipt and Processing of Information', Paragraph 2.

3.3.2.2. Public Disclosure

The Whistleblower is **entitled to** make a Public Disclosure of the Breach, benefiting from the Legal Protections, only if the following prerequisites are met (the '**Public Disclosure Prerequisites**'):

- has **first carried out the Report** (Internal and External, or directly External), but
  - ✓ **appropriate action has not been taken in** response to the Report within a period of three months from the date of receipt of the Report, or,
  - ✓ **if** no acknowledgement of receipt has been sent to the Whistleblower, 3 months from the expiry of the 7-day time limit from the date of Reporting;

or when

- the Whistleblower has **reasonable grounds to** believe that:
  - ✓ the breach may constitute an **imminent or obvious danger to the public interest**, such as where there is an emergency situation or the risk of irreversible damage; or
  - ✓ in the case of an External Report, **there is a risk of retaliation or may be ineffective due to the** circumstances of the case, such as where evidence may be concealed or

destroyed, or where there is reason to believe that the recipient of the Report may be colluding with or involved in the Breach.

3.4. Reporting Managers

3.4.1. Generalities

The management of Internal Reporting Channels and Follow-up is entrusted to the Reporting Committee composed of the following persons, who are granted an **autonomous functional position for this** purpose, and who must be **specifically trained** for this management:

- the Independent External Professional, appointed by SALVAGNINI ITALIA S.P.A.,
- the Legal Manager of the Parent Company SALVAGNINI ITALIA S.P.A.,
- the HR Manager of the Parent Company SALVAGNINI ITALIA S.P.A.,

which act collectively in the common capacity of "**Reports Committee**", unless otherwise provided for in this Procedure.

3.4.2. Budget

The body in charge of appointing the Case Managers assesses the appropriateness of/allocates to the Case Manager(s) an annual budget, which can be used for the performance of the task, provided that the Case Managers do not already have a budget for their own functioning.

3.4.3. Tasks

The Case Managers, as a body deemed impartial and competent by the companies, have the **task** of

a) receive and take charge of Reports;

b) screen alerts (see Chapters 3.5.2 and 3.6.1);

c) provide the first Notice to the Whistleblower within the time limit provided for in Chapter 3.5.4; maintain contact with the Whistleblower for subsequent communications; diligently follow up the Report;

d) if it is competent to do so, ensure the proper investigation of the reported facts, through actions such as an internal investigation, enquiries, requests for supplementary information if necessary from the Whistleblower, requests to third parties;

e) if competent for the matter, decide on the outcome (validity) of the Reports, on the basis of the results of the investigation, and communicate it to the Whistleblower within the deadlines set out in Chapter 3.5.4;

f) if competent for the matter, cooperate with the other competent corporate functions to verify that the reported breach is remedied, e.g. also through criminal prosecution, an action for the recovery of funds;

g) take care of the proper filing and storage of Reports;

h) coordinating with the Privacy Function, as well as with the designated DPO, where necessary or required, to meet the compliance requirements of the personal data processing operations covered by the Reports;

i) make available clear information on the Reporting Channels, procedures and prerequisites for making Internal and External Reports, by means of display in workplaces, publication on the Company's website or by any other means enabling Whistleblowers to access such information;

j) cooperate with the IT Manager, upon request, to ensure that the requirements for the protection of computerised Reporting Channels and the storage of Reports are met;

k) communicate to the administrative bodies of the companies to which the Reports refer, on an annual basis by 31 January, an annual report on the Reports received and their outcome; the report is not necessary if there are no Reports during the year. The report may be sub-annual if the Case Managers consider it necessary.

It is strictly forbidden for anyone to exert pressure, send instructions, attempt to condition in any form whatsoever, and in general try to compromise the autonomy, impartiality and independence of the Case Managers.

3.5. Examination of Reports

3.5.1. Switching / Protocoling

The Report received through Reporting Channels other than the Portal/Software is logged/entered immediately in the Portal/Software by the Case Manager who first receives it. This entry causes an ID Code to be assigned to the Report (protocolation).

3.5.2. Preliminary screening

Upon receipt of the Report, the Case Managers must **take charge** of it and its **preliminary assessment**, aimed at ascertaining:

- whether the Report contains the minimum mandatory information required, and is therefore to be considered admissible,
- whether the Report contains manifestly false information and should therefore be rejected immediately,
- the type of Breach reported (e.g. 231 Violations, Sectoral Violations), and
- the possible conflict of interest of the Case Manager with respect to the Report itself.

(the '**Screening**').

Reports containing clearly false or unreliable information must be rejected by the Case Managers, with the whistleblower being advised that such information gives rise to claims for damages and may be prosecuted in court or as an administrative offence.

If the Case Manager consider it to be **admissible** and also within their **competence**, they proceed with the further steps (investigation, etc., on which see below).

If, on the other hand, the Case Managers assess that the further handling of the Report is **beyond their** technical or legal **knowledge** (because it falls within the competence of other Case Managers - e.g. DPO, other legally competent subjects such as the Board of Auditors, Auditors and Auditing

Firms), they will provide for the **confidential forwarding of** the Report to such other subjects, simultaneously notifying the Whistleblowerof the transmission.
In particular, this must be done at the first available meeting or, if urgent, without delay.

The Case Managers, if deemed necessary or useful for the performance of their tasks, may delegate in writing to one or more persons (internal, in compliance with the powers vested in the delegate as per the corporate delegation system in force, or external) the performance of the investigative tasks under e) and/or f) above (e.g. if they require specialised technical or legal expertise) (the "**Co-optation**") and under a prior written obligation of strict confidentiality. To this end, the Case Managers shall ensure in advance that the delegate is aware of this procedure.

This is **without prejudice to the sole responsibility of the Case Manager(s) as regards the final decision on** the merits of the Report, as well as in relation to the measures to eliminate the consequences and causes of the reported Breach if so provided for in the company's functional organisation chart.
The Case Managers, in agreement with the Top Management, may also delegate in writing to the aforementioned third party specialist, on a case-by-case basis, the exclusive power of final decision on the merits of the Report. In such a case, the delegated third party necessarily assumes the role of Case Manager.

3.5.3. Conflict of interest

The Case Managers, if they consider the existence of a **conflict of interest** with respect to the Report they receive (*e.g. the subject of the Report concerns violations attributable to the Case Manager themselves, or to the functional area in which the Handlers perform their usual duties*), are required to

- refrain from dealing with the Report, and
- immediately transfer the handling of the Report to other Case Managers not subject to a conflict of interest, or, in the absence of such a Case Manager not subject to a conflict of interest, to the Parent Company's Statutory Board of Auditors), communicating in writing the nature of the conflict detected.

In the event of any **doubt** as to the existence of his or her conflict of interest, the Case Manager must immediately notify the other Case Managers, who will then assess the same with him or her.

The nature of the conflict detected with respect to a Report must be declared within the "notes" field in the Portal/Software, by the Case Manager not in conflict of interest.

3.5.4. Feedback to the reporter

Within 7 calendar days of receipt of the non-anonymous Report, the Case Managers shall provide the Whistleblower with an acknowledgement of receipt of the Report, via the SaaS Portal/Software, or, if the SaaS Portal/Software cannot be used, at the postal, e-mail or other electronic address indicated by the Whistleblower.

The acknowledgement of receipt may be omitted if:
- the reporter expressly opposed, or
- the Case Manager has reason to believe that confirmation of receipt of a written Report would compromise the confidentiality of the identity of the Whistleblower.

Acknowledgement to the Whistleblower on the outcome of the Report must be provided within a period of **three months:**

- from the date of the acknowledgement **of receipt of** the Report, or,
- if no initial notice was sent to the Whistleblower (e.g. because the Whistlblower remained anonymous), from the **expiry of the period of 7 days** from receipt of the Report.

NB: If **no Follow-up** (as defined in Chapter 2) of the Report **has been decided upon** at the end of this three-month period, the Whistleblower **must be informed of this, as well as** of any further feedback to be expected.

The Whistleblower using the Report ID received can access the Portal/Software and interact with the Case Managers designated from time to time by the Companies.

3.6. Investigation

3.6.1. Generalities

Each Report must be assessed for admissibility and substantive merit. The Case Manager(s) is/are not required to follow up a Report:

- which does not fall within the scope of this Procedure, or
- from which the admissibility of the same cannot be deduced.

If the Report is deemed *prima facie* **admissible**, the relevant Case Managers proceed with the investigation of the facts that are the subject of the Report. For this purpose, he/she/they will, by way of example and not limited to:

a) verify whether the companies have adopted adequate Procedures to guard against the risk of the Breach that is the subject of the Report;

b) if they deem it necessary or appropriate, request and receive further information, clarifications, and/or the production of deeds and documents from the Whistleblower - if known - or from other persons, including third parties (e.g. heads of function or any other internal or external person), in possession of information useful for the preliminary investigation, in particular, reasonably concerning the processes at risk of Breach.

[N.B.: It is not necessary for the companies adhering to this Procedure **to obtain from third party suppliers a written commitment to report** and cooperate with the Case Managers in the investigation of their respective Reports, since the Clause 231, if any, signed by the Company is already suitable to guarantee such cooperation also in relation to non 231 Violations that emerge in connection with the same operational processes to which the 231 risks refer.

(NB: *Third parties may invoke professional secrecy to which they are legally bound - e.g. legal or medical - and/or because of any previous confidentiality agreements with other third parties*)]

c) With immediate timeliness, moreover, the Case Managers receive from the Heads of the respective functional areas of the company any information they become aware of concerning:

- measures and/or news coming from judicial police bodies and/or any other competent Authority, from which it is inferred that investigations are being carried out, even against unknown persons, for Breaches;

- requests for Legal Protection made by employees or directors of the Companies in the event of legal proceedings being initiated for Breaches;
- reports prepared by the Heads of function within the framework of their control activities and from which facts, acts, events or omissions may emerge with critical profiles with respect to the reported Breaches;
- requests made by the persons reported (i.e. charged with the Infringements) in order to defend their rights allegedly infringed by the Report received.

3.6.2. Priorities

Alerts are processed in the following **order of priority**:

a) severity of the reported conduct / number of breaches reported;

b) reasons of urgency in order to prevent any further damage (e.g. to health) as a consequence of the events reported;

c) repeated commission of the facts already the subject of a previous Report;

d) involvement of several parties in the matter reported;

e) any further circumstances assessed at the discretion of the Case Manager.

3.7. Obligations to cooperate

Any person who is requested by a Case Manager to provide information and assessments in connection with a Report is obliged to cooperate diligently and to maintain the confidentiality of the content of the Information exchanged.

3.8. Archiving the Report

In the event that the outcome of the screening or subsequent more extensive investigation is found:

- the absence, even partial, of data constituting essential elements of the Report; or
- the general content of the Report is such that it does not allow the reported facts to be understood; or
- the Report is accompanied by inappropriate or irrelevant documentation; or
- unfoundedness due to the absence of concrete factual elements capable of justifying findings,

the Case Managers **declare** the Report received **inadmissible, and** consequently archive it through the Portal/Software.

Such filing is promptly **notified** through the Portal/Software:

- to the Whistleblowing (if known or otherwise reachable via the Portal/Software's Secure Inbox),
- the other Case Managers, if they were not involved in the Screening or Investigation of the Alert,
- the administrative bodies of the companies to which the Reports refer, in the periodic report by the Case Manager.

3.9. Actions following the Report

3.9.1. Unfoundedness of the Report with wilful misconduct or gross negligence

In that case, Archiving must be carried out, through of .

If the Case Manager find elements that, in their considered judgement, point to bad faith or gross negligence on the part of the Whistleblower, they shall communicate this in writing:

- to the Reported; and
- the Head of the Whistleblower's functional area, as well as the Head of HUMAN RESOURCES, for the assessment of the application of any sanctions against the Whistleblower.

3.9.2. Report confirmed by checks

In the event that, at the outcome of the investigations, the Case Manager responsible for the **merits of the Report** find that the facts of the Report are **well-founded**, they shall communicate the final outcome of the investigation in a traceable manner, for any assessment within their competence:

a) to the Reported;

b) the Head of the functional area to which the Whstleblower belongs;

c) to the Head of the functional area to which the Report refers;

d) the HUMAN RESOURCES Function; and

e) the administrative body of the Company to which the Breach relates; and

f) in the case of an external reporter:
(i) the legal representative pro tempore of the third party organisation to which the Whistleblower himself/herself belongs (or, if he/she is deemed to be in a position of conflict of interest with respect to the reported Violation, the Head of the different functional area of the third party organisation that appears competent to examine the communication), and
ii) the Head of the internal functional area of the Company that has contractual relations with that organisation;

g) to the Board of Auditors of the Parent Company;

unless such communication would hinder further investigations or judicial proceedings for the protection of the rights of the Companies; in any case, the Case Managers shall assess the advisability of delaying the aforesaid communication, depending on any confidentiality requirements during the course of the investigation.

3.9.3. Administrative, civil or criminal proceedings

In the event that the Case Manager considers that there are grounds to initiate administrative, civil or criminal proceedings (e.g. criminal complaint) against an Involved Person indicated in the Report or identified as a result of subsequent investigations, he/she shall either independently initiate such action, or inform an internal person competent to initiate such proceedings on the basis of the delegation system in force at the time, unless the latter person has a conflict of interest in relation to the Report, in which case the Case Manager(s) shall consult with the Personnel Department to identify the most appropriate Function or person to receive the request to initiate the aforementioned administrative, civil or criminal proceedings.

In the event that the internal person responsible for such performance under the delegation system in force at the time has a conflict of interest, the case manager shall inform an internal apical person who does not have a conflict of interest.

3.9.4. Non-compliance with Internal Procedures

In the event that the investigation carried out following the Report leads the Case Managers to ascertain (i) the absence of specific corporate Procedures aimed at ensuring against the risk of Breaches or (ii) the lack of adequate internal and/or external disclosure thereof, or (iii) the lack of internal training with respect to the rules laid down in the Procedure, the Case Managers shall report such circumstances to the functional heads of the Company to which the Breach refers and to the Parent Company's Legal Department, for appropriate remedies.

3.9.5. Report confirmed by verification, but indeterminate in terms of damage suffered or insufficient evidence gathered

In such cases (*examples: reports in the media; cyber fraud, cartels in public tenders, conflicts of interest and other circumstances or conduct not easily detectable by internal controls, etc.*), additional investigative activities should be assessed, with an indication of the professional expertise required (e.g. specific legal or technical expertise on the reported facts or underlying processes).

On the basis of the results of these further investigations, should the reported facts be confirmed, the actions referred to in section 3.9.2 may be pursued.
Otherwise, further legal action must be taken or reports must be made to the competent authorities for any necessary investigations.

3.9.6. Reporting on facts that are plausible but cannot be verified

In these cases, too, the actions mentioned in section 3.9.2 above can be pursued.

4. CONSERVATION

The Reports of Violations, and the related documentation, must be **archived** exclusively for the time necessary to process the Report and in any case **no longer than 5 years from the date of the documentation of the final outcome** of the Reporting procedure, and beyond this period for as long as necessary for the completion of administrative or judicial proceedings already commenced or for investigative proceedings pursuant to the Code of Criminal Procedure.

5. LEGAL PROTECTION

The Whistleblower and other Protected Persons are granted by the Companies the Safeguards set out in ***Appendix B***.

6. TRAINING

Training, communication and information activities are an indispensable component of the effective implementation of the Whistleblowing organisational model and are regulated in ***Appendix D***.

7. DISTRIBUTION

The Case Managers shall make available to the addressees of this Procedure, clear information on the Reporting Channels, the prerequisites for making Internal and External Reports and Public Disclosures, using one or more of the following methods:

- Posting in a visible place in the workplace (company notice board),
- Making available
  - ✓ hands and/or
  - ✓ by e-mail, or
  - ✓ via the company intranet or
  - ✓ via another software application (e.g. personnel and/or payroll software or procedure distribution software),
- Publication in a special section of the company website (the URL of which is communicated by the company),
- Made available via link/icon on the first electronic page of the Reporting Portal/Software.

8. SANCTIONS

Failure to comply with the provisions contained in this procedure may give rise - in addition to the civil and criminal penalties provided for by the legislation in force - to disciplinary sanctions by the Company, in accordance with the provisions of the National Collective Labour Agreement (to be understood as expressly referred to herein).

Furthermore, the Company expressly reserves the right to sanction those who are found to be responsible for the above-mentioned offences.

The following **sanctions are** also provided for:

Italy

Who

- obstructs or attempts to obstruct a Whistleblower or any other Protected Persons. in connection with any Report or puts them under pressure through deliberate judicial or administrative proceedings, or
- adopts a retaliatory act,
- violates confidentiality provisions,

commits an **administrative offence** and, unless the offence is punished with a more severe penalty by another provision of law, is punished by the ANAC - National Anti-Corruption Authority, with an **administrative fine** ranging from EUR 10,000.00 to EUR 50,000.00.

Austria

Who

- obstructs or attempts to obstruct a Whistleblower or any other Protected Persons. in connection with any Report or puts them under pressure through deliberate judicial or administrative proceedings,
- adopts a retaliatory act,
- violates confidentiality provisions, or
- knowingly provides false information,

commits an **administrative offence** and, unless the offence is punished with a more severe penalty by another legal provision, is punished by the district administrative authority with a **fine of** up to EUR 20,000.00, and in the case of a repeat offence up to EUR 40,000.00.

9. OTHER

For anything not expressly provided for in this procedure, the following applies:
- in relation to reports concerning the companies SALVAGNINI ITALIA SPA and SALVAGNINI INDUSTRIALE SPA, Decree no. 24/2023 (Whistleblowing Decree), and the further regulations referred to therein;
- in connection with reports concerning the company SALVAGNINI MASCHINENBAU GMBH, the Whistleblowers Protection Act (HSchG), and further regulations referred to therein.

APPENDIX A - SECTORAL VIOLATIONS

Sectoral Violations include:

a) **offences c**(acts and omissions, even if only attempted or concealed) **falling within the scope of the following sectoral** Union **acts**[5] :

Privacy and data protection E.g. breaches of privacy obligations such as information to data subjects, collection of consent on processing, data and processing protection measures, documentation, etc.
Environmental Protection E.g. violations of administrative prescriptions possibly punished with pecuniary administrative sanctions and falling within the perimeter of environmental offences under Legislative Decree 231/2001.
Product safety and conformity E.g. obligations to ensure the quality and safety of marketed products intended for use by the consumer public
(only in Austria) Prevention and Punishment of Crimes under Sections 302-309 of the Austrian Criminal Code (StGB), Federal Law Gazette No. 60/1974: • Article 302 Abuse of Office • Article 303 Unlawful restraint or deprivation of liberty and Unauthorised search of a dwelling • Article 304 Bribery in public acts • Article 305 Acceptance of Benefits • Article 306 Acceptance of benefits to influence • Article 307 Passive corruption • Article 307a Granting of benefits • Art. 307b Granting of benefits to influence • Article 308 Undue influence in public acts • Article 309 Bribery in private acts

b) **acts or omissions affecting the financial interests of the Union as** referred to in Article 325 TFEU specified in the relevant EU secondary legislation;

c) **acts or omissions relating to the internal market**, as referred to in Article 26(2) TFEU, including:
   1. violations of EU competition and state aid rules, and
   2. infringements concerning the internal market related to acts violating corporate tax rules (in the case of Italy: IRES, IRAP) or
   3. mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;

[5] See Annex to EU Directive 1937/2019.

d) **acts or omissions that frustrate the object or purpose of the provisions of Union acts** in the areas referred to in (a), (b) and (c).

NB. For a detailed description of these relevant areas, see the ***Annex (Part I and Part II) of the Whistleblowing Decree*** available at www.normattiva.it.

APPENDIX B - SAFEGUARDS

1. PROTECTED SUBJECTS

Protected Subjects include,

- the reporter (even anonymous, whose identity is discovered at a later stage),
- those who lodge a complaint with the judicial authorities in relation to a breach,
- those who make a Public Disclosure, and
- the following categories of persons:
  - Facilitators,
  - **Persons** in the same employment context as the Whistleblower, the person who filed a complaint with the judicial authority or the person who made a Public Disclosure and who are related to them by a stable emotional or kinship link up to the fourth degree (cousins),
  - **Work colleagues of the** Whistleblower, of the person who has filed a complaint with the judicial authority or made a Public Disclosure, who work in the same work context as the Whistleblower and who have a habitual and current relationship with that person,
  - **Entities that own, or are employers of, or operate in the same employment context as the aforementioned persons.**

2. PROTECTION

In the event of a Report, **all Protected Persons** are guaranteed the following three mandatory categories of legal protection:

- PROTECTIVE MEASURES,
- SUPPORTING MEASURES,
- RIGHT TO CONFIDENTIALITY,

as detailed below.

In addition, with regard to **Whistleblowing only**, the Safeguards also apply if the Report or Public Disclosure occurs in the following cases:

(a) **when the legal relationship** with the Companies **has not yet started**, if information on Breaches was acquired during the selection process or in other pre-contractual stages;

(b) during the **probationary period**;

(c) **after termination of the legal relationship**, if the Breach Information was acquired during the course of the legal relationship.

The **reasons** that led the person to report or publicly disclose **are irrelevant for** the purposes of Protection.

3. PROTECTIVE MEASURES[6]

[6] The protection afforded to the Whistleblower will be guaranteed only in the case of reports made by clearly identified persons. Disclosure of the identity by the Whistleblower may take place at any time even after the Report, without prejudice to the protection granted above.

The following **Protection Measures** apply to Protected Persons:

- Prohibition of Retaliation,
- Protection from Retaliation,
- Limitations of liability,
- Waivers and conditional settlements.

NB: Protective Measures also apply:

(a) in cases of anonymous Report or Public Disclosure, if the Whistleblower was subsequently identified and retaliated against, and

b) in cases of External Report submitted to the competent institutions, bodies, offices and agencies of the European Union (*e.g. the European Anti-Fraud Office*), in accordance with the conditions for External Report themselves.

3.1. Prohibition of retaliation

Protected Persons may not be subjected to any Retaliation (meaning *any conduct, act or omission, even if only attempted or threatened, carried out by reason of the Report or Whistleblowing or Public Disclosure and that causes or may cause the Whistleblower, directly or indirectly, unjust damage)* (**prohibition of retaliatory acts**).

Retaliation' is to be **understood broadly**, including **but** not limited to;

(a) **dismissal**, **suspension** or equivalent measures;

(b) downgrading or **non-promotion**;

(c) change of duties, **change of place of work**, **reduction of salary**, **change of working hours**;

(d) **suspension of training** or any restriction of access to it;

(e) **demerit notes or negative references**;

(f) the adoption of **disciplinary measures** or other sanctions, including fines;

(g) **coercion**, **intimidation**, **harassment** or **ostracism**;

(h) **discrimination** or otherwise **unfavourable treatment**;

(i) **failure to convert** a fixed-term employment contract into an employment contract of indefinite duration, **where the employee had legitimate expectations of** such conversion;

(j) **non-renewal** or **early termination of** a fixed-term employment contract;

(k) **damage**, including to a person's reputation, particularly on social media, or **economic or financial loss**, including loss of economic opportunities and loss of income;

(l) inclusion on improper lists (e.g. **black lists**) on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;

m) the **early** termination (termination) or **cancellation of the contract for the supply of goods or services**; **the introduction of detrimental changes** to the service or supply contract;

(n) **cancellation of a licence or permit;**

(o) a request to undergo **psychiatric or medical examinations**.

3.2. Protection from Retaliation

3.2.1 Reporting to Public Authorities

In Italy

Whistleblowers may **report to the ANAC any retaliation they believe they have suffered**.

In order to acquire preliminary elements that are indispensable for ascertaining the retaliation, the ANAC may avail itself of the cooperation of the Civil Service Inspectorate and of the INL, within the limits of their respective competences, without prejudice to the exclusive competence of the ANAC as regards the assessment of the elements acquired and the possible application of administrative sanctions.

In Austria

Whistleblowers may report **retaliation they believe they have suffered to the BAK**.

3.2.2 Invalidity of acts and restoration of the previous situation

In Italy

In the event of non-application or non-observance, even partial, of the Safeguards by the Companies, the Protected Person may invoke, even cumulatively:

- The **nullity ex lege of the acts of retaliation**, resulting in the re-establishment of the situation prior to them.
- **Reinstatement in the** employee's job in accordance with the legislation applicable to the employee, if the Protected Person has been dismissed because of the Report.

In Austria

The Company to which the retaliatory act is attributable for a justified Report must

- restore the ex ante rule of law,
- compensate pecuniary damage and
- pay compensation for any personal damage suffered by the Whistleblower.

3.2.3 Burden of Proof

In Italy

In the context of judicial or administrative proceedings or extrajudicial disputes concerning the ascertainment of the conduct, acts or omissions, constituting prohibited Retaliation, it shall be presumed that the same have been committed as a result of the Report or Public Disclosure.

The burden of proving that they are motivated by reasons unrelated to the Report or Public Disclosure lies with the person who has carried them out.

In the event of a **claim for damages submitted to the judicial authorities by the** Whistleblower (and not, therefore, by other Protected Persons), if the plaintiff proves that he/she has made a Whistleblowing Report or a Public Disclosure under the Whistleblowing Decree and has suffered damage, it **shall be presumed, unless proven otherwise, that the damage is a consequence of such** Whistleblowing **Report or Public Disclosure**.

In Austria

The burden of proof regime is regulated in Austria in an opposite manner to that in Italy, as follows.

In judicial or administrative proceedings in which a Whistleblower claims to have been harmed by an act of retaliation as a consequence of a Report, the onus is on the Whistleblower to prove that the act was taken in retaliation for the Report.

It should not be presumed that the act was taken in retaliation for the Report if, when all the circumstances are assessed, it is more likely than not that another motive was decisive for the act. The link between the act and the Report must therefore be reasonably proven by the Whistleblower.

3.3. Limitations of liability

The Whistleblower shall not be criminally liable, and any further civil or administrative liability, for the disclosure or dissemination of Breach Information is also **excluded:**

- breaches covered by **secrecy** obligations (official, business, professional, scientific, commercial or industrial) (punishable by Articles 326, 622, 623 of the Criminal Code),
- copyright infringements,
- **personal data protection** (privacy) violations,
- violations that offend the reputation of the person involved or reported (Reported)

provided, however, that **there were reasonable grounds for believing that the disclosure or dissemination of the same Information was necessary** to disclose the Breach and the Report, Public Disclosure or the Judicial Report.

The above-mentioned criminal, civil and administrative exemption, however, does not apply:

a) in the event that the Whistleblower commits an **offence in order to acquire or access the Information** that is the subject of the Report.
E.g., the offence of unauthorised access to a computer system exists in relation to the act of a person who intentionally hacked into the e-mail system of a work colleague in order to obtain evidence in support of a report, and

b) **for conduct, acts or omissions not related to** the Report, Judicial Report or Public Disclosure or not strictly necessary to disclose the Breach.

The Companies may also impose **disciplinary sanctions against** persons who decide to retaliate, in accordance with the following documents:

- National Collective Labour Agreement (therefore to be understood as expressly referred to herein).

3.4. Prohibition of transactions (Italy only)

The rights and protections provided for in favour of the Signatory **may not be waived or settled, in whole or in part,** which shall therefore be deemed invalid, unless they are made in the form and manner provided for in Article 2113(4) of the Italian Civil Code.

4. SUPPORTING MEASURES

In Italy

The Whistleblower is entitled to **support measures** consisting of **free information, assistance and counselling** on the modalities of Whistleblowing and on the protection from retaliation offered

by national and European Union law provisions, on the rights of the Whistleblower, and on the terms and conditions of access to legal aid.

These support measures are provided by Third Sector Entities that have entered into agreements with ANAC. The list of such Third Sector Entities is published on the website: https://www.anticorruzione.it/-/whistleblowing.

Such free information, assistance and advice may be requested at any time by the Whistleblower from these Third Sector Bodies, even before the actual communication of the Report.

In addition, the reporter with an income below certain thresholds is entitled to free legal aid in civil and administrative proceedings, in accordance with the relevant legislation (see link https://www.giustizia.it/giustizia/it/mg_3_7_2.page#).

In Austria

Legal aid is regulated in Austria as follows.

In connection with Reports concerning the company SALVAGNINI MASCHINENBAU GMBH, the Whistleblower and other Protected Persons are entitled to legal aid in criminal and civil proceedings, provided they are entitled to legal aid in accordance with the provisions of the Code of Criminal Procedure and the Austrian Code of Civil Procedure.

Professional associations (legal representatives of professionals) are authorised, in individual cases, to grant support to the extent necessary to avoid the difficulties caused by legal costs in defending against acts of retaliation against the persons concerned, if and to the extent that there is no entitlement to the benefits of legal aid or legal protection by a legal representative of interests or by private or group legal protection insurance.

5. CONFIDENTIALITY

5.1. Generalities

Reports may not be used beyond what is necessary to adequately follow them up.

The non-anonymous Whistleblower must be guaranteed confidentiality by either the Companies, the Case Managers and anyone else involved in receiving and processing a Report, about:

- **His identity and** that of **persons close to him facilitating** the Report (right to anonymity), throughout the entire Reporting process, to anyone other than the Case Manager[7], and
- **the content of the Report**, including the **documentation** attached thereto, to the extent that its disclosure, even indirectly, might allow the identification of the Whistleblower.

At all stages of the activity, it is forbidden to **reveal the identity** of the Whistleblower to **the Involved Person or to other persons not expressly authorised, without** express **consent** of the Whistleblower.

The Internal Reporting Channels adopted by the Company must therefore guarantee the aforementioned confidentiality.

5.2. Exclusion of confidentiality

[7] Confidentiality also covers all other information from which the identity of whistleblowers can be deduced directly or indirectly.

The obligation of confidentiality does **not apply** in the following cases:

(i) when the **disclosure of** the identity of the Whistleblower is a **necessary and proportionate obligation** imposed by Union or national law **in the context of investigations by** national authorities **or judicial proceedings**, including for the purpose of safeguarding the rights of defence of the person reported.
For this purpose**, the person reported must be warned without delay by the Handlers of the Report of an unfounded Report made in bad faith or with gross negligence against him/her in** order to be able to assess whether to exercise any rights against the person reported[8]; or

(ii) the existence of an obligation to communicate the name of the reporter to the **judicial or police authorities**, or

(iii) any **voluntary waiver in** writing of confidentiality at any time by the reporter, or

(iv) if knowledge of the identity of the Whistleblower is indispensable for the **accused's defence**, only if the Whistleblower has expressly consented to the disclosure of his/her identity.

In any case, the Whistleblower **must be informed in writing** by the Handlers of the Report or by the competent authority of the reasons for **disclosing** confidential data **before his/her identity is disclosed**, unless this would prejudice the relevant investigation or judicial proceedings[9] .

The Companies, the Case Managers and anyone else involved in the receipt and processing of a Report must also protect **the identity of the Involved Persons and of the other persons mentioned in the Report** until the conclusion of the proceedings initiated on account of the Report, in compliance with the same guarantees of confidentiality provided for in favour of the Whistleblowing.

6. PREREQUISITES FOR PROTECTION. UNFOUNDED, BAD FAITH OR GROSSLY NEGLIGENT REPORTING

Protection Measures apply when the following **conditions** are met:

(a) at the time of the Report or Complaint to the Judicial Authority or Public Disclosure, the Whistleblower had **reasonable grounds to believe that the Information about the Violations** reported or publicly disclosed **was true** and fell within the objective scope of Section 2.3;

(b) the Report or Public Disclosure was made on the basis of the provisions of this procedure.

The Protection of Protected Subjects also exists in the event of a **Report or Disclosure that later turns out to be unfounded**, if the Whistleblower, at the time of the Report or Public Disclosure,

---

[8] In order to allow the reported person to file a complaint-complaint (even against unknown persons) for the offence of slander, defamation or other offences that can be proven in the specific case, and also in view of the fact that the reported person may entrust a lawyer with the task of carrying out 'preventive defensive investigations' (pursuant to Articles 327 bis and 391 nonies of the Code of Criminal Procedure, institutes that may also serve the person unjustly accused of a crime to identify the identity of the person who made an anonymous report against him/her).
On the other hand, the protection of the Whistleblower's confidentiality must be ensured where he/she is not in bad faith; indeed, the purpose of 'whistleblowing' could be frustrated if it were expressly provided that the Whistleblower must be informed of an unfounded but not in bad faith report, especially in the case of minor negligence (not punishable even at disciplinary level, but theoretically - although it is rare - actionable in civil law).

[9] When informing the Whistleblower, the competent authority shall send him/her a written explanation of the reasons for disclosing the confidential data in question.

had **reasonable grounds to believe that the Report was necessary to disclose the Breach** and the Report or Public Disclosure or report to the judicial authority that the Information was within the scope of this Procedure.

Safeguards in favour of the Protected Subjects are not guaranteed, and a disciplinary sanction is also imposed on the Whistleblower, when it is **established, even by a judgment of first instance,**

i) **the criminal liability of** the Whistleblower for offences of slander or defamation in relation to the facts reported, or

ii) the Whistleblower's **civil liability, for the** same reason (pursuant to Article 2043 of the Civil Code, which provides for the right to compensation for damages in favour of anyone who is the victim of an extra-contractual damage caused by a third party), in cases of **wilful misconduct or gross negligence**.

Reports made in the **knowledge of** the **abuse/exploitation of** the Reporting procedure, e.g. those that are manifestly unfounded, **opportunistic** and/or made for the **sole purpose of harming** the reported person or other persons mentioned in the Report (employees, members of corporate bodies, suppliers, partners, group companies, etc.) shall be considered in **bad faith/grievous misconduct** (and therefore a source of liability, in disciplinary and other competent fora).

In the event of a **Public Disclosure,** the Whistleblower benefits from Legal Protection if, in addition to the basic condition, one of the Public Disclosure Prerequisites laid down in Chapter 3.3.2.2 of the Procedure is also fulfilled.

APPENDIX C - PROCESSING OF PERSONAL DATA

1.1 Any processing of personal data carried out for the purpose of handling the Report must be carried out in accordance with the legislation on the protection of personal data (GDPR, Supervisory Authority's Measures, Legislative Decree 196/2003)[10] .
Accordingly, anyone involved in the receipt and processing of non-anonymous Reports **is required to comply with all the procedures, protocols and written security instructions laid down in the** Company's **privacy system**, without prejudice to the further rules laid down in this procedure.
It is understood that the Companies' ***Privacy Policy*** on Whistleblowing is to be considered as a procedure, containing specific rules on data processing, compliance with which by the Companies is essential to ensure compliance of processing with the requirements of the GDPR and the Whistleblowing Decree.

1.2 **Personal data that appear to be not reasonably relevant and useful for the processing of a specific Report shall not be collected or, if received or collected accidentally, shall be promptly deleted by** the relevant Case Manager(s) with respect to the Breach.

1.3 The aforementioned processing operations must be carried out by the Company (data controller) **in compliance with the general principles set out in Articles 5[11] and 25[12] of the GDPR,** and by taking appropriate measures to protect the rights and freedoms of the data subjects.

1.4 The LEGAL Function, in coordination with the IT Function:

- defines, by means of this procedure and its annexes, the model for the receipt and management of Internal Reports, identifying technical and organisational measures suitable for ensuring a level of security appropriate to the specific risks arising from the processing operations performed,

---

[10] E, by the competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, of Directive (EU) 2016/680.
11 1. Art. 5 GDPR: Personal data are:
(a) processed lawfully, fairly and transparently in relation to the data subject ('lawfulness, fairness and transparency');
(b) collected for **specified, explicit and legitimate purposes,** and subsequently processed in a way that is not incompatible with those purposes ('purpose limitation');
(c) **adequate, relevant and limited to what is** necessary in relation to the purposes for which they are processed ('data minimisation');
(d) **accurate** and, where necessary, **kept up to date**; all reasonable steps must be taken to delete or rectify in a timely manner data that are inaccurate in relation to the purposes for which they are processed ('accuracy');
(e) **kept in a** form which permits identification of data subjects **for no longer than the purposes** for which they are processed ('limitation of storage');
(f) processed in such a way as to **ensure appropriate security of** personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage ('integrity and confidentiality')
12 Art. 25 GDPR: Article 25 Data protection by design and data protection by default
1. Taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of the processing, and taking into account the risks to the rights and freedoms of natural persons represented by the processing which are likely and likely to vary in severity both when determining the means of the processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, such as pseudonymisation, to implement effectively the principles of data protection, such as minimisation, and to integrate in the processing the necessary safeguards in order to meet the requirements of this Regulation and to protect the rights of data subjects.
2. The controller shall implement **appropriate technical and organisational measures** to ensure that only personal data necessary for each specific purpose of the processing are processed by default. This obligation shall apply to the amount of personal data collected, the scope of the processing, the storage period and the accessibility. In particular, these measures ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person.

- carries out the Data Protection Impact Assessment (DPIA) carried out by the Privacy Function itself, and
- governs the relationship with any external suppliers that process personal data on behalf of the Company(s) pursuant to Article 28 of the GDPR (e.g., external Case Manager(s) designated by the Company, third-party Portal/Software Managers);
- provides, and/or identifies the different corporate functions responsible for providing, appropriate information to the Whistleblower and the Persons concerned (pursuant to Articles 13 and 14 of the GDPR).

1.5 The Case Managers ensure that Internal Reporting Channels other than the 'Portal/Software' are set up and operated in a secure manner that guarantees the confidentiality of the identity of the Whistleblower and of any third parties named in the Report and the protection of the Report from the risk of unauthorised access, loss of integrity and/or availability.

The security measures applied to the Portal/Software are set out in the Contract between the Companies and the third party provider of the same, and in the relevant documentation, including ***Admin Manuals*** and ***Case Manager Manuals (Appendix E)***.

Configuration of the basic functionality of the Portal/Software is the responsibility of the designated Admin role(s), while technical maintenance is the responsibility of the third-party provider of the Portal/Software (EQS/Adacta).

1.6 This Procedure also represents, pursuant to and for the purposes of Article 13, paragraph 5 of the Whistleblowing Decree, an internal agreement between the Companies of SALVAGNINI Group, aimed at

i) regulate the **sharing of resources** (e.g. Portal/Software) for the receipt and management of Reports and

ii) determine their respective **responsibilities with** regard to compliance with data protection obligations, pursuant to Article 26 of the GDPR, as follows:
   - **Privacy Policy**: Each company acts as a co-processor with regard to the processing of data related to:
     - **sharing the** internal reporting **channel** consisting of the Saas Integrity Line Portal/Software; and
     - the **Whistleblowing Procedure** for the communication/collection and management of reports.
   - **information to interested parties pursuant to Art. 13** GDPR:
     a) The privacy notice to Whistleblowers is made available to the data subject by the relevant Whistleblower Managers, as follows:
        - ✓ by means of a special link/text viewable on the landing page, if the reporter (even anonymous) **uses the Portal/Software** to send the Report;
        - ✓ by hand-delivery, at the earliest opportunity, in the case of a **personal meeting** with the Whistleblower not preceded by the use of the Portal/Software for sending the Report;
        - ✓ if the Whistleblower **telephones** the Company to make the Report: by means of a verbal notice to the Whistleblower about the availability of the Information on the Portal/Software;

- ✓ by means of a specific document/link/viewable hypertext made available within the Secure Inbox, if the **Report is anonymous** and reaches the Company by an **offline** means (e.g. by registered letter with return receipt) and is then **entered autonomously in the Portal/software by the person receiving the Report;**

b) the privacy notice to the Involved Subjects (natural persons to whom the reported Breach is alleged) is made available to the data subject by the CAse Managers, in the following manner:

- ✓ by hand delivery, at the earliest opportunity, in the case of a **personal meeting** with the person concerned;
- ✓ by means of a specific link/text viewable on the landing page, if the Involved Party **uses the Portal/Software** to interact with those evaluating the Report;
- ✓ in the event that the contact with the Involved Party is made by **telephone**: by verbal notice to the Whistleblower of the availability of the Information Notice on the Portal/Software;

- **response to the exercise of the data subject's rights**: each company acts as an independent data controller, in accordance with its own procedures for handling the exercise of data subjects' rights, to which reference is made here;
- **personal data breaches**: each company acts as an independent data controller in accordance with its own data breach management procedures, to which reference is made here ;
- **security measures**: each Group Company is required to comply with the security measures provided for i) in this Procedure, ii) in the functional specifications of the Portal/Software, ii) in its privacy system, iv) in the data protection legislation applicable to it;
- **Operational interface with the third party provider of the Portal/Software**: the Parent Company acts as the centralised technical interface to the provider, on behalf of the other companies, on the basis of a mandate with representation to be understood as conferred herein.

APPENDIX D - TRAINING

Training, communication and information activities (i) represent an indispensable component for the effective implementation of the Whistleblowing organisational model, (ii) constitute proof of the real will of the entity to be an active part of the prevention of the offences subject to whistleblowing, on the other hand, (iii) stimulate the cooperation of individuals in the effective realisation of the objective of legality.

The person in charge of this Procedure must make easily accessible to the entire organisational structure - in a manner differentiated according to the role of the users - clear information about, at the very least, the prerequisites and procedures for reporting Violations, the Protections afforded to whistleblowers and the limits of such Protections.

The HUMAN RESOURCES Department, in agreement with the Head of this Procedure, draws up and periodically updates a ***Whistleblowing Training Plan*** which forms an integral part of this Appendix.

APPENDIX E - PORTAL/SOFTWARE MANUALS

- ***Admin User Manual***
- ***User Case Manager Manual***
- ***Synoptic table "Manual Entries" vs "Privileges/accesses in the back-end".***