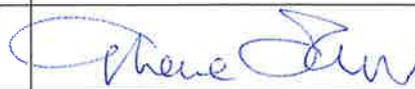


WHISTLEBLOWING PROCEDURE

CREATED	ADACTA ASSOCIATED FIRM (AVV. LUCA DE MURI)	
CONTROLLED	AVV. GIULIA CHIARA PAOLONI	
APPROVED	Dr. FRANCESCO SCARPARI	
Protocol referent <i>Responsible for storage, updating, dissemination and application</i>	AVV. GIULIA CHIARA PAOLONI	
VERSION	2.0	
DATE	09.02.2026	
VERSION NOTES	<ul style="list-style-type: none"> • Added clarifications on certain types of reportable Violations • Inserted new Violations relating to AML / self laundering • Inserted additions regarding the replacement of temporarily incapacitated Case Managers • Integrations regarding internal assignment of report management • Integrations regarding conflict of interest and coordination of the clause with the possibility of external reporting to ANAC • Clarifications regarding the alternation of oral reporting channels • Integrations for the case of receipt of reports sent by the reporter by e-mail • Supplements for the case of receipt of the report by more than one person, some of whom are not competent • Supplements on the consequences of the inadmissibility of the report • Supplements regarding the assessment of whether the preconditions for the protection of the whistleblower are met • Supplements on the possibility of using the investigation service of the parent Company in groups of companies • Clarifications on information flows from the Case Manager to senior bodies • Clarification on feedback to the Whistleblower within 3 months from the date of the report • Clarifications regarding the transfer of decision-making power on the report to parties other than the original Report Managers • Clarification on whistleblowing training • Supplement on lessons learned • Clarification on co-ownership agreement for the processing of personal data in groups of companies (Annex C) • Clarification on the Whistleblower's dialogue with ETS - third sector entities 	

	<ul style="list-style-type: none">• Additions regarding the deadline for the deletion of personal data 5 years after the final decision and for Austria and Germany	
--	---	--

Index

Index.....	3
1. PURPOSE	4
2. DEFINITIONS AND SCOPE OF APPLICATION	4
2.1. Definitions	4
2.2. Subjective scope of application.....	8
2.3. Objective scope.....	10
3. REGULATION OF ACTIVITIES	11
3.1. Generalities.....	11
3.2. Object of the Report.....	11
3.3. Types of Report	12
3.4. Handlers of Reports.....	16
3.5. Examination of Reports.....	19
3.6. Investigation	22
3.7. Archiving the Report unfounded without malice or gross negligence.....	27
3.8. Other actions following the Report	27
4. CONSERVATION	30
5. LEGAL PROTECTION	31
6. TRAINING	31
7. DISTRIBUTION	31
8. SANCTIONS.....	32
9. OTHER	33
10. CHANGES.....	33
APPENDIX A - SECTORAL VIOLATIONS.....	34
APPENDIX B - PROTECTIONS.....	38
APPENDIX C - PROCESSING OF PERSONAL DATA	48
APPENDIX D - TRAINING.....	51
APPENDIX E - PORTAL/SOFTWARE MANUALS.....	52

1. PURPOSE

This procedure governs¹ the ways in which the Companies, as legal entities in the private sector, fulfil their obligation to establish a system for handling Whistleblowings (channels, procedures, resources) and to guarantee Whistleblowers the Safeguards provided for by law and by the procedure itself, in accordance with

- the relevant legislation DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report Violations of Union law (hereinafter, the "**Whistleblowing Directive**"), and
- to D.Lgs. 24/2023,
- the ANAC Guidelines, and
- (in Austria) to the Whistleblower Protection Act (HinweisgeberInnenschutzgesetz - '**HSchG**').
- (in Germany) to the Hinweisgeberschutzgesetz (**HinSchG**)

The procedure is intended to facilitate the correct implementation of EU 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. The Companies also handle Whistleblowings to avoid incurring detrimental effects related to Violations (e.g. negative publicity on the market).

The purpose of this Procedure is to **ensure professional, confidential, impartial processing and adequate protection of the rights of the data subject** during the entire process of making, handling, processing, investigating and resolving Reports made through the Company's Internal Reporting Channel.

This Procedure regulates the roles, processes and means of operation of the Company's Internal Reporting Channel, so as to **regulate matters relating to Reports made by Whistleblowers, as well as their management and resolution by** the Case Manager.

The procedures for the processing, investigation and resolution and, in general, the management of the Reports received pursuant to this Procedure shall be governed by the utmost **objectivity and independence**, establishing in this Procedure the corresponding mechanisms in order to avoid the concurrence of possible conflicts of interest.

Furthermore, the rights to be informed of the actions or omissions attributed and the presumption of innocence of the Involved Person are guaranteed by this Procedure.

2. DEFINITIONS AND SCOPE OF APPLICATION

2.1. Definitions

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

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) the best practices applicable in this field (ISO 37002).

ANAC - Autorità Nazionale Anticorruzione (or Competent Authority)	<i>Italian independent administrative authority designated to i) receive External Reports and ii) perform the functions provided for by the Directive, including feedback to the Whistleblower, in particular with regard to the Follow-up given to the Reports, in the cases provided for by the Whistleblowing Decree.</i>
Violations of Sectorial Acts	<i>conduct, acts or omissions which harm the public interest or the integrity of the Companies and which 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 whether:</i> <ul style="list-style-type: none"> - <i>the employment relationship with the Companies has ended in the meantime (so-called former employee), or that</i> - <i>the facts have been learnt during the selection process (e.g. candidate) or in other phases of pre-contractual negotiations with the Companies</i> <i>irrespective of whether, under national law, Whistleblowing violations are administrative, criminal or violations of purely civil law (e.g. risk of damages).</i>
Administrative sanctions	<i>Administrative pecuniary sanctions applicable by ANAC in cases of non-compliance provided for therein, or (ii) by another Public Authority in cases of non-compliance provided for by local whistleblowing legislation</i>
ANAC Guidelines	<ul style="list-style-type: none"> • <i>ANAC Guidelines on the protection of persons who report violations of Union law and the protection of persons who report violations of national laws - Procedures for the submission and management of external reports (approved by resolution No. 311 of 12 July 2023 - Outline of new guidelines on whistleblowing 07 November 2024), and</i> • <i>Regulations for the management of external whistleblowing and for the exercise of ANAC's sanctioning power in implementation of Legislative Decree 24/2023 (approved by Resolution No. 301 of 12 July 2023).</i>
BAK	<i>Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung, i.e. Federal Office for the Prevention and Combating of Corruption, see website: http://www.bak.gv.at/</i>
Company	<i>The Companies indicated in Chapter 3.2.1 below</i>
Disciplinary sanctions	<i>Disciplinary sanctions applicable by the Companies in the event of non-compliance with the provisions of this Procedure</i>
External Parties	<i>Whistleblowers other than Internal Parties</i>

External Reporting	<i>communication, written or oral, of Breach Information by the Whistleblower submitted through the Reporting Channel activated by ANAC or other competent public Authority in accordance with the whistleblowing legislation applicable from time to time to the Report</i>
Facilitator	<i>A natural person who assists a Whistleblower in the Whistleblowing process, operating within the same work context and whose assistance shall be kept confidential, including a trade unionist if he/she assists the Whistleblower in his/her name and on his/her behalf, without using his/her trade union code.</i>
Follow-up	<i>action taken by the Whistleblowing Manager to assess the existence of the facts reported, the outcome of the investigation and any measures taken</i>
GDPR	<i>EU Data Protection Regulation 679/2016</i>
Group	<i>The corporate group to which the Company(ies) belongs</i>
HSchG	<i>HinweisgeberInnenschutzgesetz (Federal Act on the Protection of Whistleblowers, which implemented the Whistleblowing Directive in Austria, 01.02.2023 in force since 25.02.2023)</i>
HinSchG	<i>Hinweisgeberschutzgesetz (Federal Law Gazette 2023 I No. 140) of 31 May 2023, in force since 2 July 2023, which implements the Whistleblowing Directive in Germany</i>
Independent External Professional	<i>The external subject (natural or legal person), autonomous and trained, other than the Supervisory Board 231 and the Data Protection Officer, designated by one or more Companies as the Case Manager.</i>
Information on Violations	<i>Information, including reasonable suspicion, concerning: (i) Violations committed or which, based on concrete evidence, could be committed in the organisation with which the Whistleblower or the person making the complaint to the judicial or accounting authorities has a legal relationship, and (ii) elements concerning possible conduct aimed at concealing such Violations</i>
Internal Persons	<i>Whistleblowers defined as internal in the table in paragraph 2.2.3 of this procedure</i>
Internal Reporting	<i>written or oral communication of Breach Information, submitted through the Reporting Channels made available by the Companies</i>
Legal relationship	<i>Legal relationship between the Whistleblower and the organisation where 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))</i>

Portal/Software	<i>the third-party cloud portal, accessible on the Internet at https://salvagnini.integrityline.com, which can be used by the reporter to perform an Internal Reporting</i>
Private Sector subjects	<i>Subjects, other than those falling within the definition of Public Sector Subjects</i>
Procedure	<i>This document and its Appendices</i>
Procedures	<i>set of directives, instructions, protocols and written procedures provided for and implemented by the Company in order to prevent Violations, and/or to reduce their consequences or recurrence</i>
Protected Persons	<i>The persons envisaged in paragraph 1 of Appendix B of this Procedure, who may benefit from the Protections</i>
Protection measures	<i>Measures provided for in paragraph 2 of Appendix B of this Procedure</i>
Public Disclosure	<i>making information about Violations publicly available through the press or electronic media or in any case through means of dissemination capable of reaching a large number of people (e.g. radio, television, blogs, internet, automated e-mail campaigns)</i>
Public Sector Persons	<i>public administrations referred to in Article 1(2) of Legislative Decree No. 165/2001 public economic entities bodies governed by public law referred to in Art. 3, co. 1, lett. d), Legislative Decree 50/2016 public service concessionaires, publicly controlled companies referred to in Art. 2, co. 1, lett. m) of Legislative Decree 175/2016, even if listed, in-house companies referred to in Art. 2, co. 1, lett. o) of Legislative Decree 175/2016, even if listed</i>
Redress	<i>Communication to the Whistleblower of information on the follow-up that is given or that is intended to be given to the Report.</i>
Register of Reports	<i>software in which to register the Reports</i>
Reporting Channels	<i>channels for the execution of the Reporting, 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 are in turn defined as Internal or External depending on whether they are managed directly by the Companies or respectively by third parties authorised by them</i>
Reporting Committee	<i>Collegial body composed, for each Company, of: - the Independent External Professional, - the Legal Manager of the Parent Company SALVAGNINI ITALIA S.P.A, - the HR Manager of the Parent Company SALVAGNINI ITALIA S.P.A;</i>

	<i>- any additional Case Managers appointed from time to time by the Company</i>
"Case Manager"	<i>person(s) designated by the Companies to receive the Report and carry out the further related activities provided for in Chapters 3.4.3 and 3.5 of this Procedure</i>
Retaliation	<i>any conduct, act or omission, even if only attempted or threatened, committed by reason of the Whistleblowing or Report to the Judicial Authority or Public Disclosure and which causes or may cause the Whistleblower or the person making the Report, directly or indirectly, unjust damage</i>
Safeguards	<i>the set of Protection and Support Measures provided by the Whistleblowing Decree</i>
Sectorial Acts	<i>regulatory acts identified in Appendix A of this Procedure</i>
Involved Person (Reported)	<i>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</i>
Support measures	<i>measures envisaged in paragraph 6 of Appendix B to this Procedure</i>
TFEU	<i>Treaty on the Functioning of the European Union</i>
Third Sector entities	<i>Entities that have entered into agreements with ANAC to provide support measures under their competence pursuant to the Whistleblowing Decree. They never take on the role of Facilitator</i>
Whistleblower	<i>natural person, as indicated in Chapter 2.2.3., who makes the Report or Public Disclosure of Information on Violations acquired in the context of his/her own Work Context</i>
Whistleblowing Decree	<i>D.L.gs. 24/2023 implementing the Whistleblowing Directive in Italy</i>
Whistleblowing Directive	<i>EU Directive 2019/1937 on the protection of persons who report Violations of Union law</i>
Whistleblowing Privacy Policy	<i>Information communicated pursuant to articles 13-14 of the GDPR by the Company to the Interested Parties</i>
Work context	<i>Work or professional activities, present or past, carried out in the context of legal relations, through which, regardless of the nature of such activities, a person acquires information on Violationss and in the context of which he/she could risk to suffer Retaliation in case of a Report or Public Disclosure or a report to the Judicial Authority</i>

2.2. Subjective scope of application

2.2.1. This Procedure applies to the following Companies:

- ✓ **SALVAGNINI ITALIA S.P.A.**, with registered office in Via 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**, with operational headquarters at Dr. Guido Salvagnini-Straße 1, 4482 Ennsdorf – Austria,
- ✓ **SALVAGNINI DEUTSCHLAND GMBH**, with operational headquarters at Am Surbach 1, 35625 Hüttenberg - Germany,

(the "**Companies**").

From time to time, this Procedure will specify if different and/or additional rules to those in force in Italy apply in relation to Reports concerning SALVAGNINI MASCHINENBAU GmbH or SALVAGNINI DEUTSCHLAND GmbH.

2.2.2. In relation to the aforesaid 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 foreseen in **Appendix A**,
- to other Protected Subjects;
- to other Interested Subjects who are involved in various ways in the Follow-up to Reports.

2.2.3. Whistleblowers may belong to the following categories:

ID	Subject Category	Subject Nature
A	Employees of the Companies, including workers performing occasional services, regardless of the position they hold within the Company, the legal nature of their relationship and the area of activity or hierarchical level.	Internal Party
B	Paid and unpaid volunteers and trainees working for the Company	Internal Party
C	Self-employed workers, including self-employment relationships that are subject to special rules pursuant to Article 2222 of the Italian Civil Code (work contracts) (including freelancers and consultants working for the Companies), <i>e.g. intellectual professions for the exercise of which registration in special registers or lists is required, such as psychologists, architects, surveyors, etc.</i>) as well as Holders of a collaboration relationship referred to in Article 409 of the Italian Code of Civil Procedure , who perform their work activities for the Companies, by which is meant 1) those of private subordinate employment, even if not inherent to the exercise of a business; 2) agency, commercial representation relationships; and 3) other collaborative relationships resulting in the provision of continuous and coordinated work, mainly personal, even if not of a subordinate nature	External Party

	<i>e.g. lawyers, engineers, social workers, who provide their work for the Company by organising it autonomously (para-subordinate relationship)</i>	
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 Company	External Party
E	Shareholders	External Party
F	Members of the administrative and/or management or representative body 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 Party
G	Members of the control or supervisory body of the Companies (e.g. Auditors, Auditors or Auditing Company, DPO - Data Protection Officer)	Statutory Auditors: Internal Party; Auditor or contact person of auditing company - DPO: External Party

2.3. Objective scope

Whistleblowers are required to provide information on well-substantiated Violations based on precise (adequately detailed) and concordant factual elements, and not on facts that are generic, confusing and/or manifestly defamatory or slanderous.

The following will not be taken into account, and will result in exclusion from the Safeguards under this Procedure

a) **challenges, claims or requests linked to an interest of a personal nature of the Whistleblower or of the person making a complaint to the judicial authorities that relate exclusively to their individual employment relationships, or inherent to their employment relationships with hierarchically superior figures.**

(e.g. Reports concerning labour disputes, discrimination between colleagues, interpersonal conflicts or involving only the Whistleblower and another worker or the persons to whom the Public Disclosure or Complaint relates), and

b) **information contained in Reports that have already been rejected** by any Internal Reporting Channel or by the ANAC, and

c) **information already fully available to the public** or which constitutes mere **hearsay**, and

(d) information referring to **acts or omissions not expressly covered** by this Procedure.

The Reports **may also be anonymous**, i.e. they may not bear the identity of the Whistleblower or allow for reconstruction or retrieval. They will be examined, provided they meet the above requirements.

This is without prejudice to:

(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 shall always be entitled, in the event that he/she has information about an offence, to lodge a complaint with the competent criminal authority).

All Reports sent through the Internal Reporting Channel shall be made in good faith. This means that, at the time of submission, the Whistleblower shall have reasonable and sufficient grounds to believe that the information provided is true, accurate and has not been obtained through potential violations (e.g. criminal offences).

In this sense, **malicious or grossly negligent reporting may give rise to the relevant sanctions by the Company**, without prejudice to the civil and criminal liabilities that may ensue.

3. REGULATION OF ACTIVITIES

3.1. Generalities

Reporting is:

- a) **mandatory** – except in Germany and Austria, where it is optional – on the part of **Internal Whistleblower** (NB. by virtue of the **general duties of loyalty, diligence and good faith** connected to the legal relationship with the Companies, to be understood as expressly reaffirmed herein);
- b) **mandatory**, on the part of **External Parties** who **are contractually obliged** towards the Companies to report;
- c) **optional**, on the part of **External Parties** of the Companies who are not contractually obliged towards the Companies to report.

3.2. Object of the Report

In order to facilitate and allow the necessary checks and investigations by the Companies, also to verify the validity of the Report, the Whistleblower is advised to provide at least the **following**:

- the **identity of the Whistleblower** (name, surname, tax code, position or function held), unless he/she decides not to proceed with an anonymous Report;
- **relationship with the Company** (candidate, employee/collaborator, director, shareholder, supplier/consultant, partner, etc.) and, if applicable, position/qualification/company position of the Whistleblower;
- a description of the **reasons** related to the work activity carried out that allowed the knowledge of the reported facts;
- a clear, detailed and complete **description of the facts that are** the Involved Person;
- **the circumstances of time and place** in which the facts were committed, if known;
- **the personal details** of the person to whom the breach is attributed or useful elements for identifying him/her, if known;
- an indication of any **other persons who may report** on the facts that are the Involved Person;

- an indication of any **documents** that may confirm the validity of the facts that are the Involved Person;
- any other **information** that may provide useful feedback on the existence of the facts reported;
- if applicable, a **communication's channel** with the Whistleblower other than the Portal/Software (e-mail address, telephone or other) so that the Reporting Committee can communicate with the Whistleblower.

If, having assessed the content of the Report, it turns out to lack the minimum mandatory requirements for its proper assessment, the Reporting Committee will proceed to request the corresponding information and/or documentation from the Whistleblower through the communication methods indicated by the latter, proceeding as per Chapter 3.5.2 in case the necessary information is not available for the opening of the investigation phase.

3.3. Types of Report

A **Report** is defined as:

- a) **Internal**, if directed to the Companies² ; in which case it may be made 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 performed **to the competent authority**,
- c) **Public disclosure** if made in the presence of the specific prerequisites provided for by the Whistleblowing Decree for the latter.

3.3.1. Internal Reporting Channels

The Internal Reporting Channels shall 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.

3.3.1.1. Communication of Whistleblowing

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

- ✓ **COMPUTERS:**
 - **Portal/Software³** , which can be reached at <https://salvagnini.integrityline.com>,
- ✓ **ORAL:**
 - Voice **recording** (on a registered message/voice mailbox) possible in the Portal/Software.

² The Reporting Party shall first check whether it is possible to communicate the Breach Information by means of an Internal Reporting, 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 only allowed in the cases strictly provided for.

³ The instructions for the use of the Portal/Software by the Whistleblower can be found on the first online page of the Portal/Software.

Case Managers are obliged to document the Oral Report by means of a **detailed account of** the conversation **written** by the staff handling the Report.

- o *(at the request of the Whistleblower)* **Direct personal meeting** with one or more Case Managers, also by remote session via videoconference.

The Case Managers ensure in this case, **subject to the necessary consent of** the Whistleblower, 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 by means of:

- b) **an audio recording of the conversation on a durable audio medium** allowing access to the Information; or
- c) **a detailed** and complete record of the meeting and the conversation conducted.
- d) **transcription/upload and storage of the said minutes on the Portal/Software.**

If the Whistleblower has disclosed his/her identity, or, in the case of an anonymous Whistleblowing, this is also possible without disclosing identity, the Case Managers shall give the Whistleblower the opportunity to **verify, rectify and approve** the said minutes by his/her signature.

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

3.3.1.2. Communication of the Report

Report to erroneous subject

If a person other than the competent Report Managers receives a Report, he/she shall transmit it to the competent Report Managers, within 7 (seven) days of its receipt, complete with any supporting documentation received, not retaining any copy and refraining from taking any independent initiative for analysis and/or investigation, and guaranteeing its confidentiality at all times.

Failure to communicate 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 per paragraph 9 below.

If the content of a Report becomes known to persons other than the Report 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 Report Managers.

Reporting to more than one internal person

In the event that **the Report is sent, at the same time, to more than one person, all internal** to the Company, the Report shall be considered as sent to a non-competent person. Therefore, the person or persons in charge of receiving such Reports should forward them, within 7 days from their receipt to the competent internal subject, simultaneously notifying the Whistleblower.

Reports also sent to several external subjects

If, on the other hand, **the Report is sent not only to the internal subject in charge of handling it, but also to several persons** outside the institution, the Whistleblower should be asked for clarification of the circumstances that led to the Report, in order to ascertain whether the Whistleblower intended to proceed directly to public disclosure.

In such a case, given that there are no conditions for considering that the internal Reporting was carried out correctly (since the Whistleblower has chosen not to address only and exclusively the internal person responsible for handling the report), it is necessary to understand whether the Reporting can be qualified as a Public Disclosure and to ascertain whether or not one of the conditions set out in Article 15 of the Whistleblowing Decree is met.

3.3.2. External Reporting and Public Disclosure

3.3.2.1. External Report

The Whistleblower can only make an External Report if one of the following **conditions** is met when submitting it:

- a) no Internal Reporting Channel has been mandatorily set up within its work context; or
- b) the Internal Reporting Channel, even if theoretically envisaged as compulsory by the Companies, **is not in fact active or, even if activated, does not comply with** the regulatory indications;
- c) the Internal Reporting already carried out by the Whistleblower **has not been followed up⁴**;
- d) the Whistleblower has **well-founded reasons to believe** that, if he/she were to make an Internal Report, it would not be effectively followed up or that the Report could give rise to the **risk of retaliation**;
- e) the Whistleblower has reasonable grounds to believe that the Breach may constitute an **imminent or clear danger to the public interest**.

In Italy

External Reporting is made to ANAC:

- **in writing** through the Reporting Channel activated by ANAC.
(for more information on contacts and instructions on the use of the External Reporting Channel, on the confidentiality regime applicable to External Reports and on the process for handling External Reports see the website <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

In relation to information concerning Violations concerning the Company SALVAGNINI MASCHNINENBAU GmbH, the External Reporting of Violations for the different types of bribery provided for in **Appendix A** can be made to the "Single Point of Contact (SPOC) for Corruption and

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

Abuse of Authority" established at the **Federal Office for Preventing and Combating Corruption** (BAK - Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung, website: <http://www.bak.gv.at/>)⁵, by:

- regular mail to: BAK - Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung - Herrengasse 7 - 1010 Vienna – Austria;
- telephone +43 1 53 126-906800;
- fax +43 1 53 126-108583;
- e-mail .BMI-III-BAK-SPOC@bak.gv.at.

Although the reporter always has the possibility to remain anonymous, it is good practice to provide at least an address, because in many cases more detailed information is needed to carry out investigations. In many cases, under the rules governing criminal and police investigations, it may be indispensable to reveal the source of the report, even if it is made anonymously.

The BAK is not competent to the extent that other federal authorities or agencies are responsible for information on violations of law.

A list of such other federal authorities and bodies can be found in the Federal Act on the Procedure and Protection of Whistleblowers (HSchG), Section 3, Article 'External Bodies for the Receipt and Processing of Information', Paragraph 2.

In Germany

The whistleblower may also submit an external report to an external reporting centre. Whistleblowers should give priority to reporting to an internal reporting office in cases where effective internal action can be taken against the violation and they do not fear retaliation. If an internally reported violation has not been resolved, the whistleblower is free to contact an external reporting centre.

External reporting centres include, for example Federal Office of Justice, Adenauerallee 9-103, 53113 Bonn (<https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundesnode.html>);

Federal Financial Supervisory Authority (BaFin), Whistleblower Reporting Centre, Graurheindorfer Straße 13e 108, 53117 Bonn

(https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html);

Federal Cartel Office, Kaiser-Friedrich-Straße 13e 16, 53113 Bonn (https://www.bundeskartellamt.de/SharedDocs/KontaktDaten/DE/Externe_Meldestelle.html).

⁵ The BAK is not competent insofar as other federal authorities or agencies are responsible for information relating to violations of the law.

Section 15 HSchG and other regulatory provisions identify the following authorities as external reporting channels:

- Federal Anti-Corruption Office
- Auditor Oversight Authority – pursuant to the Auditor Oversight Act
- Accounting Authority – pursuant to the Accounting Act
- Federal Competition Authority – pursuant to the Competition Act
- Financial Market Supervisory Authority – pursuant to the Financial Market Supervisory Authority Act
- Money Laundering Reporting Office – pursuant to the Federal Criminal Police Office Act
- Notary chambers – pursuant to the Notary Act
- Austrian Bar Association – pursuant to the Disciplinary Statute for Lawyers and Trainee Lawyers
- Chamber of Tax Consultants and Auditors – pursuant to the Professional Law on Accountants and Tax Consultants

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**"):

- **it has first made the Report** (internal and external, or directly external), but
 - ✓ **appropriate action has not been taken** in response to the Report within a period of 3 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 the Report.

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 not be effective** 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. Handlers of Reports

3.4.1. Generalities

The Board of Directors is the competent body for the appointment, as well as for the removal or dismissal, of the Whistleblowing Manager, who, in turn, is responsible for the management and processing of Whistleblowing that enter the Internal Reporting Channel.

The Case Manager may be a natural person or a collegiate body that may delegate to one or more of its members (natural person) the powers to manage and process individual Reports.

In case SALVAGNINI ITALIA SPA appoints a Case Manager assigning him/her, through this Procedure, the competence to manage also Reports concerning other Companies of the SALVAGNINI Group, such appointment is meant to be carried out also in the name and on behalf of the Board of Directors of the beneficiary Company, on the basis of a mandate to carry out the appointment itself automatically given by the same Company to SALVAGNINI ITALIA SPA through the acceptance of this Procedure.

The management of the Internal Reporting Channels and of the Follow-up is entrusted to the Reporting Committee composed of the following subjects, who are guaranteed for this purpose a **functional position autonomous and independent** from the rest of the corporate functions and from the hierarchical or functional subordination that may exist. It is composed of:

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

who collectively act as the "**Reporting Committee**", unless otherwise provided for in this Procedure.

In the remainder of this Procedure, the reference to the "Case Managers" or to the "Reporting Committee" is to be understood as limited to the sole Whistleblowing Manager, in case the latter remains such according to the rules laid down therein.

In the event that the only Case Manager initially designated operates the possible Investigation Delegation provided for in Chapter 3.6.3.1.d, or in the event of the designation of more than one Case Manager, they act collectively as the 'Reporting Committee', and any reference to the Case Manager shall be understood as referring to the 'Reporting Committee'.

Without prejudice to the generality of the foregoing, it is therefore strictly forbidden for any person to exert pressure, send peremptory instructions, attempt to condition or hinder in any form whatsoever, and in general try to compromise the autonomy, impartiality and independence of the Reporting Committee.

Each member of the Reporting Committee **shall be specifically trained** for such management. It is essential that the choice falls on a person who has all the knowledge and skills for an effective management of the Whistleblowing.

It is preferable that it is a person with a good knowledge of law, ethics and integrity, and who has been adequately trained in the processing of personal data and whistleblowing.

The Case Manager shall be guaranteed adequate knowledge of the Company's functional organisation chart.

The Case Manager who is temporarily absent or unable to perform his or her duties (due to holidays, illness, accident), shall report this to the other members of the Reporting Committee. Moreover, in the event of a holiday, if the Report Portal does not allow automatic notification of receipt of the Report to the Whistleblower within the strict deadline of 7 days from the date of the Report, and the Report Manager cannot be temporarily replaced by other Report Managers, he/she shall give formal notice to potential Whistleblowers on the home page of the Portal/software, indicating the duration of the holiday.

3.4.2. Budget

The body responsible for appointing the Alert Managers assesses whether it is advisable to/should allocate them an annual budget, to be used for the performance of the task, provided that the Case Managers do not already have a budget for their own operation.

3.4.3. Tasks

The Reporting Committee, as a body considered impartial and competent by the companies, are in **charge of:**

- a) receive and take charge of Reports;
- b) Screening the Reports (see Chapters 3.5.2 and 3.6.1);
- c) **provide the first Notice** to the Whistleblower within the time limit set out in Chapter 3.5.4; maintain contact with the Whistleblower for subsequent communications, unless this may compromise the confidentiality of the Report or the identity of the Whistleblower or the Whistleblower has waived the right to use the communications relating to the investigation; diligently follow up the Report;
- d) **diligently follow up** the Report;

- e) determine, in coordination with area Company contact persons if necessary, the advisability or necessity of taking immediate action to **prevent** (stop or mitigate) **further damage**;
- f) if competent for the matter, take care of the proper investigation of the reported facts, through actions such as an internal enquiry, investigations, requests for additional information if necessary from the Whistleblower, requests to third parties;
- g) decide on the outcome (merits) of the Reports, on the basis of the results of the preliminary investigation, and communicate it to the Whistleblower within the deadlines set out in Chapter 3.5.4;
- h) **propose the appropriate measures for the resolution of the Breach, as well as, where appropriate, the disciplinary measures** to be taken, with the possibility of delegating this power to another competent body;
- i) **communicate the outcome of the Report to the relevant persons** within the deadline set out in this Procedure (unless, in the case of the Whistleblower, he/she has waived the right to avail himself/herself of the communications relating to the investigation);
- j) ensure that Reports are properly **filed** and **stored**;
- k) **coordinating with the Privacy Function**, as well as with the DPO that may have been designated, where necessary or required, to meet the compliance requirements of the processing of personal data subject to the Reports;
- l) **provide clear information** on 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;
- m) **manage the Internal Reporting Channels, guaranteeing the necessary protection requirements** of the system for managing and storing data on Reports, also by limiting access to them, also **by making use of the competences and activities of the Company's IT and/or Privacy Functions**, without prejudice to the responsibilities and powers of the latter deriving from the Company 's system of delegated powers;
- n) **communicate to the Board of Directors** of the companies to which the Reports received relate, 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.
- o) **resolve any doubts and requests for clarification** concerning the provisions of this Procedure;
- p) keep the Whistleblowing Register up-to-date;
- q) ensure that appropriate measures are taken to **prevent and avoid possible retaliation** against the Whistleblower and other Protected Persons. To perform the aforementioned tasks, and in cases where it deems it necessary, the Reporting Committee may be assisted by an external consultant or even delegate to the latter some of the aforementioned functions. In this respect, the Reporting Committee will have to obtain a confidentiality agreement from the external consultants involved in the management and resolution of the communication.

Likewise, he shall obtain the same from internal collaborators, when he deems it useful or necessary.

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 shall **take charge of** the Report and its **preliminary screening**, aimed at ascertaining that the Report:

- contains the minimum mandatory Information required, and is therefore to be considered admissible,
- **concerns facts constituting a type of Breach** included among those listed in **Appendix A**,
- originates from **Whistleblowers belonging to one of the categories set out** in this Procedure,
- contains Information that is patently false, and shall therefore be immediately rejected,
- does not contain **Information** that already on summary examination appears **to be the result of an offence committed by the Whistleblower**,
- does not appear, already on summary examination, to have been made by the Whistleblower in **bad faith**, i.e. with the intention of harming the Company or third parties connected to it
- **does not contain any significant new information** on the Violations **with respect to a previous Report** for which the relevant decisional procedure has been completed,

(the '**Screening**').

Reports containing demonstrably false or unreliable information shall be rejected by the Case Managers, with a warning to the Whistleblower that such information gives rise to claims for damages and may be prosecuted in court or as an administrative offence.

The Reporting Committee will have to issue a **decision as to whether or not** the Report **can be prosecuted**.

The Reporting Committee if it assesses that the Report **is unreviewability**:

- **shall refrain from further pursuing an Report;**
- issues a decision to **dismiss** the Report on grounds of unreviewability under the Whistleblowing Decree, **giving reasoned written notice**;
 - **to the Whistleblower**, unless the latter has waived the right to receive communications;
 - **to the Board of Auditors**.

In the event that the Reporting Committee during the Screening detects the possible absence of the conditions required by the Whistleblowing Decree to guarantee the Whistleblower the Safeguards to

which he/she is normally entitled, it will give written notice thereof, not only to the Whistleblower, but also to the Involved Person and to the other competent internal subjects, as better indicated in chapter 3.9.1 below.

Alternatively, **if the documentation is missing or defective in any way**, the Reporting Committee may not file the Report but, if it considers it necessary, request information from the Whistleblower.

If the Case Managers consider that the Report is **admissible** and also falls 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 shall promptly **forward** the Report to such other subjects, giving simultaneous notice of the transmission to the Whistleblower.

In particular, such forwarding should take place at the first useful 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 Company's 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 '**Investigation Task**') 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.

The Case Managers remain solely responsible for the final decision as to whether the Report is well-founded, as well as for the measures to eliminate the consequences and causes of the reported Breach, whether so provided for in the Company's functional organisation chart.

The Case Managers, in agreement with the Board of Directors, may also delegate in writing to the aforementioned third-party specialist, on a case-by-case basis, the exclusive power to make the final decision on the merits of the Report. In this case, the delegated third party necessarily takes on the role of the Case Manager.

When the Report **is manifestly unfounded and there are, in the opinion of the Reporting Committee, reasonable grounds to believe that it was obtained through the commission of an offence**, in addition to inadmissibility, the Company assesses whether to send the Public Prosecutor's Office a detailed report of the facts alleged to be an offence (such a report is an obligation if the offence is prosecutable *ex officio*).

The Reporting Committee shall immediately forward the information to the Board of Directors (if there is no conflict of interest, in which case it is forwarded directly to the other competent body on the basis of the Company's system of delegated powers) for any decision on whether or not to forward it immediately:

- to the Public Prosecutor's Office **when the facts may be suspected of constituting a criminal offence**, or
- to the European Public Prosecutor's Office **when the facts concern the financial interests of the European Union**.

Finally, the Reporting Committee shall forward the communication without delay to the authority, body or third-party body that may be considered competent *ratione materiae* to handle the Report.

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 Involved Person concerns violations attributable to the Handlers 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 process 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 Board of Auditors, communicating in writing the nature of the conflict detected,
- immediately devolve the handling of the Report to another Case Manager(s) not subject to a conflict of interest, within the Reporting Committee, or, in the absence of such a Case Manager(s) not subject to a conflict of interest, to the additional person to be designated and appointed without delay by the competent Board of Directors. In the event of a conflict of interest of the competent Board of Directors, the appointment of the Case Manager will be made by the HR Manager, after consulting the Chairman of the Board of Auditors.

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

The nature of the conflict detected with respect to a Report shall be declared in the 'notes' field in the Portal/Software, by the Case Manager(s) not in conflict of interest.

In the event that no Case Manager not in conflict of interest can be identified, the Whistleblower will be entitled to make an External Report (i.e., direct to the ANAC).

3.5.4. Reply to the Whistleblower

3.5.4.1 Acknowledgement of receipt

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, to the postal, e-mail or other electronic address indicated by the Whistleblower.

The acknowledgement of receipt may be omitted if:

- a. the Whistleblower expressly objects, or
- b. the Case Manager has reason to believe that confirmation of receipt of a written Report would compromise the confidentiality of the Whistleblower's identity.
- c. the Whistleblower has not provided an address to which to communicate the acknowledgement and cannot be reached anonymously via the Portal/Software.

In case c) the report received shall be declared inadmissible by the Reporting Committee.

3.5.4.2 Acknowledgement

Acknowledgement of the outcome of the Report shall be provided to the Whistleblower within a period of **3 months**, starting:

- 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 Whistleblower remained anonymous), **from the expiry of the period of 7 days** from the receipt of the Report.

NB: If **no follow-up** (as defined in Chapter 2) to the Report **has been decided** at the end of this 3-month period, **the Whistleblower should be informed of this**, as well as of any further feedback to be expected.

NB: The time limit of three months is not, by law, binding on the Whistleblower. Exceptions, however, shall be reasonably justified by the Reporting Committee.

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

3.6. Investigation

3.6.1. Generalities

Each Report deemed to be procedural as above shall be screened to verify its procedurality and merits.

The results of the Screening are used by the Reporting Committee to determine the scope of the investigation (see e.g. point 8.3 ISO 37008) and to define an investigation plan (see e.g. point 8.4 ISO 37008).

If the Report is deemed *prima facie* **admissible**, the competent Case Managers proceed with the investigation of the facts that are the Involved Person.

To this end he/she/they, by way of example but not limited to:

- a) verify whether, in order to protect the risk of the Breach that is the Involved Person, the Companies have adopted adequate Procedures in advance;
- 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.: Third parties may invoke professional secrecy to which they are bound by law - e.g. legal or medical - and/or by reason of any previous confidentiality agreements with other third parties)

- c) verify whether, to protect against the risk of the Breach that is the Involved Person, the Companies have adopted adequate Procedures in advance;
- d) assess whether the Report **falls within the competence *ratione materiae* of other bodies or functions on the basis of mandatory provisions of law** (e.g. Board of Auditors or Auditing Firm/Auditor in administrative, fiscal, accounting and balance sheet matters subject by law to their control, RSP, DPO) and therefore, **on the basis of a decision** to be taken in agreement with such bodies and functions;
- e) **they transfer the management of the Follow-up to such bodies or functions, or share with such bodies or functions the management of the Follow-up, with the consequent assumption by them of the status - concurrent or exclusive, as the**

case may be - of Case Manager and of the consequent duties and responsibilities, subject to acceptance of this Procedure;

- f) **(in the case of their competence *ratione materiae* under this Procedure or under the corporate system of delegation of powers in force, e.g. privacy delegate, etc.) coordinate the management of the Follow-up with such bodies or functions,** subject to acceptance of this Procedure, **with the Reporting Committee retaining its original duties and responsibilities.**

In particular, such forwarding shall take place at the first useful meeting or, if urgent, without delay;

- g) **assess** that the further handling of the Whistleblowing **does not fall within the competence - on the basis of mandatory legal provisions or the delegation system - of any other Company body or function,** and consequently:

- ✓ **proceed with further** investigative **tasks** (investigation, etc.), or
- ✓ In the exceptional event that the Report Managers consider that, due to the extreme technical specialisation of the subject matter of the Report, which requires highly specific specialist skills, they are unable to diligently perform their role in accordance with this Procedure, **they shall identify, subject to agreement with the competent Administrative Body, a different competent entity** in relation to the Report, **confidentially and without delay** transferring **to the latter the management of the Follow-up, including the final decision** on the merits of the Report, subject to acceptance of this Procedure by the new entity identified as above, and simultaneously notifying the Reporting Person of the transfer.

The other body identified must meet the requirements set out in this Procedure.

- h) Assess the appropriateness of **taking immediate measures to prevent further damage** and, if necessary, implement them.

3.6.2. Priority

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

- a) seriousness of the reported conduct / number of Violations reported;
- b) reasons of urgency to prevent any further damage (e.g. to health) as a consequence of the reported facts;
- c) repeated commission of the facts already the subject of a previous Report;
- d) involvement of different subjects in the fact that is the Involved Person;
- e) any further circumstances assessed at the discretion of the Case Manager.

3.6.3. Investigation

3.6.3.1 General

Once the Report has been admitted for processing, the Reporting Committee proceeds with the investigation of the facts that are the Involved Person, carrying out all the acts, procedures and checks necessary and aimed at verifying the truthfulness of the facts that are the Involved Person, in compliance with the principles and rules set out in this Procedure.

To this end, he/she shall, by way of example but not limited to

- a) verifies whether the Company has adopted adequate Procedures to protect against the risk of the Breach that is the Involved Person;
- b) if he deems it necessary or appropriate, requests and receives further information, clarifications, and/or the production of deeds and documents from the Whistleblower - if known - or from other persons (e.g. heads of function or any other internal or external person) in possession of useful information for the preliminary investigation, in particular, reasonably concerning the processes at risk of Breach;
- c) has direct and timely access to the Company's Board of Directors and control bodies (e.g. Board of Auditors, Auditing Firm/Auditors, DPO if designated, etc.);
- d) where deemed necessary, it may **delegate in writing to one or more** (internal/external) **persons** with adequate competences the performance of the aforesaid **investigative tasks sub a-b-c**) - within the limits of the powers vested in the delegate in accordance with the corporate delegation system in force (the "**Investigative Delegation**") and subject to the delegate's commitment to comply with this Procedure.

In this case, the delegating Reporting Committee **retains** the power to:

- Assessing the results of the preliminary investigation and **making a final decision on the merits of the Report**, and
- Assessment, as far as possible on the basis of the outcome of the preliminary investigation, as to the possible **existence of wilful misconduct or serious misconduct on the part of the Whistleblower and/or of any involved persons**, as a **non-binding opinion** addressed to the function or body competent to manage the disciplinary or sanctioning proceedings against the Whistleblower or the Involved Person).

It is understood that the person to whom the Reporting Committee intends to delegate the above-mentioned activities shall report to the Reporting Committee any preventive situations of his workload that may cause the risk of a non-diligent Follow-up of the Report by the delegate *in pectore*.

3.6.3.2 Professional defence

The Reporting Committee shall assess whether it would be useful to discuss with the competent functions of the Company whether it would be useful to engage a lawyer to conduct the investigation, in the light of the legal principle of the so-called legal privilege⁶ which protects the confidentiality of communications between the assisted party and his lawyer, preventing them from being disclosed to third parties (e.g. the Public Prosecutor) or used against the assisted party in judicial or investigative proceedings.

3.6.4. Obligations to cooperate

⁶ Protection is enshrined

- by Article 103 of the Code of Criminal Procedure (secrecy of defendant-assisted communications),
- by Article 200 of the Code of Criminal Procedure (secrecy of lawyer-client communications),
- by professional secrecy (arts. 622 and 623 of the criminal code) and by the lawyer's deontological duty of confidentiality
- from the right of defence and cross-examination.

The personnel and any other internal and/or external contacts of the Company are required to **cooperate loyally and with the utmost diligence** in the investigative activities carried out by the Reporting Committee.

The internal personnel supporting the investigative activities shall have signed the prior appointment as authorised persons pursuant to Article 29 of the GDPR.

3.6.5. Collection, storage, analysis and review of electronic data

The collection, preservation, analysis and review of data in electronic format by the Reporting Committee shall comply with the legal rules on computer checks on employees and electronic evidence, under penalty of, inter alia, unusability of electronic evidence in labour and civil law.

3.6.6. Interviews

It is recommended that the Reporting Committee conduct interviews in accordance with the relevant good practice (e.g. point 8.9 ISO 37008).

3.6.7. Coordination between parent company and subsidiaries

Through the single platform (Portal/software) shared between the Companies adhering to this Procedure, **the Whistleblower can freely identify, by using the autonomous sub-channel expressly available on the screen, the Company to which he intends to make the Report.**

If the **Report is addressed to the parent Company**, the latter will receive and manage the Report, and may, if it deems it appropriate, avail itself of the support of the subsidiary to which the Report refers, after informing the Whistleblower and in compliance with confidentiality obligations.

If, on the other hand, **the Report is addressed to the subsidiary**, it is handled as follows:

a) **Subsidiaries up to 249 employees**: the receiving Company, where deemed appropriate, may avail itself of the investigative capacity (of the case manager(s)) of the parent Company, after having informed the Whistleblower.

b) **Subsidiaries with more than 249 employees**: the recipient Company shall autonomously manage the Report, without - therefore - being able to avail itself of the assistance (of the case manager(s)) of the parent Company⁷.

In both cases, the obligation to maintain contact and provide information on the development of the Report to the Whistleblower lies solely with the individual subsidiary to which the Report refers.

3.6.8. Rights of the Involved Person

In the course of the investigation, the Involved Person shall be informed of the Report with a brief account of the acts or omissions attributed to him/her and has the right to be heard at any time. This communication shall be made at a time and in a manner deemed appropriate by the Reporting Committee, according to its prudent discretion, to ensure the proper conduct of the investigation.

This information may be withheld during the hearing of the Involved Person, if it is considered that its prior disclosure may facilitate the concealment, destruction or alteration of evidence.

Without prejudice to the right to lodge written complaints, the investigation shall include, where possible, an interview with the Involved Person, in which, always in full respect of the presumption

⁷ However, this prohibition can be overcome, on a practical and formal level, if the subsidiary has separately designated a natural person coinciding with an external case manager designated by the parent company. In essence: the prohibition at issue here relates exclusively to the use of internal case managers within the parent company.

of innocence, he/she is invited to explain his/her version of the facts and to provide the evidence he/she deems appropriate and relevant.

In order to guarantee the right of defence of the Involved Person, he/she shall have access to the file (without revealing information that could identify him/her) and may be heard at any time. He/she shall also be informed of the possibility of being assisted by a lawyer.

In addition, the investigator shall listen to all the Involved Person and any witnesses and shall carry out all the procedures he/she deems necessary (examining documentation, obtaining information from external sources, etc.). The intervention of the witnesses and Involved Person shall be strictly confidential.

The investigator may also obtain any information and documentation he deems appropriate from any area or department of the organisation to corroborate the investigation.

Of all the acts of investigation and, in particular, of the explanations or statements provided by the Involved Person in the investigation of the Report, a written record shall be drawn up (provided that their prior consent has been obtained), which shall be duly signed by the Involved Person in order to certify its content and the conformity of their statements.

In the event that the presence of the Involved Person during the period of investigation may jeopardise the conduct of the investigation or the strict observance of the guiding principles of the procedure set out in this Procedure, the Involved Person may be granted, on the proposal of the investigator and by the competent corporate function, paid leave from work, without loss of remuneration, in order to ensure that the necessary investigative activities can be carried out without interference that could be detrimental to the person under investigation. Paid leave will be granted for the time necessary to carry out the investigative activities, but may in no case extend beyond the duration of the investigative process.

If the Reporting Committee deems it appropriate, the presence of external legal advisers is permitted at hearings and/or statements of the parties concerned, witnesses, etc.

3.6.9. Information flows to senior bodies

In order to guarantee the autonomy of the Reporting Committee, the Board of Directors is prohibited from deciding whether and how to follow up the Whistleblowing, requesting information, supervising the investigation carried out and/or taking decisions on the merits of the Report and the Reporting Committee.

3.6.10. Finalisation of the investigation

An investigation cannot be considered substantially complete if it does not reach the following results:

- the Reporting Committee is prepared to make findings supported by evidence, and these findings are sufficient for the Board of Directors to make a decision on the incident of non-compliance;
- the Reporting Committee is able to fully account for its work product;
- the result of the investigation provides a sufficient basis for initiating the necessary corrective action.

3.6.11. Reporting Decision and Investigation Report

Upon completion of all investigative actions, the Reporting Committee prepares a written report containing at least the following content (the '**Investigation Report**'), which is intended to be limited to the defined scope of the investigation:

- A statement of the relevant facts (descriptive information about the Report) together with the identification code of the Report and the date of registration.
- The actions taken to verify the plausibility of the facts and the limitations and constraints encountered during the investigation.
- The conclusions reached in the investigation and the evaluation of the proceedings and supporting evidence.
- The actions taken (if any).

3.6.12. Corrective measures

The Investigation Report **may also contain any proposals for potential corrective measures or improvements** to be implemented on the basis of the results of the investigation to minimise the impact of the Violations (so that the root causes of the Violations are appropriately, sufficiently and effectively addressed) and to **improve the internal controls of the Company's compliance programme** and/or proposed disciplinary measures.

The Company function(s) assigned to the policies or procedures corresponding to the breach should design a **remediation plan based on the Investigation Report**.

If requested, the Reporting Committee should report to the Company's compliance function to assist in developing an interim remediation plan. The plan should clearly state the compliance gaps or vulnerabilities and the objective(s) the measures are intended to achieve.

3.7. Archiving the Report unfounded without malice or gross negligence

In the event that the outcome of the extensive preliminary investigation is found to be unfounded due to the absence of concrete factual elements capable of justifying investigation, the Case Managers **declare the Report unfounded** and consequently archive it in the Portal/Software, promptly **informing:**

- to the Whistleblower (if known or anyway reachable through the Secure Inbox of the Portal/Software),
- to the Involved Person, only if the same has participated in the investigation;
- to the Company's Board of Directors to which the Reports refer, in the event of a periodical report by the Case Manager.

3.8. Other actions following the Report

After the issue of the Investigation Report, the Reporting Committee takes one of the following decisions.

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

In this case, the Reporting Committee rejects the Report and proceeds to dismiss it.

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

- to the Whistleblower, expressly warning him/her of the consequences under the law (absence of Safeguards);
- to the Involved Person; and
- to the Whistleblower's functional area manager, as well as to the Human Resources Manager, for the assessment of the application of possible sanctions against the Whistleblower.

3.8.2. Report confirmed by the checks carried out

In the event that, at the outcome of the investigations, the Case Managers who are responsible for the **merits** of the Report find that the facts which are the Involved Person 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 Involved Person;
- b) the manager of the functional area to which the Whistleblower belongs;
- c) to the manager of the functional area to which the Report refers;
- d) the Human Resources Function; and
- e) the Board of Directors of the Company to which the Breach refers; and
- f) in the case of an external Whistleblower:
 - to 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 Breach, to the Head of the different functional area of the third-party organisation that appears competent to examine the communication); and
 - to 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 disclosure would hinder further investigations or judicial proceedings for the protection of the Company's rights; in any case, the Case Managers shall assess the appropriateness of delaying the aforesaid disclosure, depending on any confidentiality requirements during the course of the investigation.

For Germany

However, the identity of the whistleblower must be protected and not disclosed. Information about the identity of a whistleblower or other circumstances that allow conclusions to be drawn about the identity of this person may be passed on to the competent body of the authority

- in criminal proceedings at the request of the prosecuting authorities;
- on the basis of an order in administrative proceedings following a report, including administrative fine proceedings;
- on the basis of a court decision;
- by the Federal Financial Supervisory Authority as an external reporting office in accordance with Section 21 to the competent specialist departments within the Federal Financial Supervisory Authority and, in the case of transactions referred to in Section 109a of the

German Securities Trading Act, to the bodies referred to in Section 109a of the German Securities Trading Act, or

- by the Federal Cartel Office as an external reporting office pursuant to Section 22 to the competent specialised departments within the Federal Cartel Office and, in the cases of Section 49 (2) sentence 2 and (4) and Section 50d of the Act against Restraints of Competition, to the respective competent competition authority.

In addition, information about the identity of the whistleblower may only be disclosed if the disclosure is necessary for follow-up measures and the whistleblower consents to the disclosure.

3.8.3. New Violations

If, following the investigation, **other facts are discovered which might constitute new irregularities** (whether or not falling within the scope of the Whistleblowing Decree) presumably committed by the same Involved Person or by other persons, the Reporting Committee shall, **ex officio, open a new file** (in which case the related Follow-up will take place in accordance with the applicable corporate procedures on internal investigations), and in the second case, in accordance with this Procedure) **or**, if it is related to what is being investigated in the current Whistleblowing file, **to the extension of the investigation file itself**, whether it deems it more discretionary (in which case the relevant Follow-up will take place in accordance with this Procedure only where this appears necessary for a unified handling of the matter).

3.8.4. Administrative, civil or criminal proceedings

In the event that the Reporting Committee considers that there are grounds to initiate administrative, civil or criminal proceedings (e.g. a criminal complaint) against a 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 subject 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 Reporting Committee shall consult with the Human Resources Function 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 person responsible for such fulfilment on the basis of the Company's delegation system in force from time to time is in conflict of interest, the Case Manager shall inform an internal apical person not in conflict of interest (i.e. specific Director or Auditor).

The Company will consider whether it should make a self-report to the authorities, e.g. to reduce liability or to exonerate itself, or to protect any of its own rights that may have been infringed; in order to assess the legal consequences, it may consider seeking professional legal advice, in line with point 3.6.3.2 of this procedure.

The Reporting Committee shall immediately transmit the information to the Board of Directors (provided that there is no conflict of interest, in which case the transmission is made directly to the other competent body on the basis of the Company's system of delegated powers) for any decision on whether to transmit it immediately:

- to the Public Prosecutor's Office **when the facts may be suspected of constituting a criminal offence**, or
- to the European Public Prosecutor's Office **when the facts concern the financial interests of the European Union**.

3.8.5. Improvement actions

In the event that the investigation carried out following the Report leads the Case Managers to ascertain:

- The absence of specific corporate Procedures aimed at ensuring against the risk of Breaches, or
- the lack of adequate internal and/or external disclosure of the same, or
- the lack of internal training with respect to the rules laid down in the Procedure,

the Case Managers report such circumstances to the Functional Managers of the Company to which the Breach refers and to the Parent Company's Legal Function, for appropriate remedies.

3.8.6. Report confirmed by verifications, but undetermined in terms of damage suffered or insufficient evidence gathered

In such cases (*e.g.: reports appearing in the media; cyber fraud, cartels in public tenders, conflicts of interest and other circumstances or conduct not easily detectable by internal controls, etc.*), it is necessary to assess additional investigative activities, indicating the professional expertise required (e.g. specific legal or technical expertise on the facts reported or on the underlying processes).

On the basis of the results of these further investigations, if the reported facts are confirmed, the actions referred to in point 3.9.2 may be taken.

Otherwise, further action shall be taken for legal protection or reporting to the competent authorities for any necessary investigations.

3.8.7. Report of facts that are plausible but cannot be verified

In these cases too, the actions referred to in point 3.9.2 above may be taken.

3.8.8. Referral

The Reporting Committee may decide to refer the report to the authority, body or third-party body considered competent to deal with it (e.g. FIU).

Whatever the decision, it shall be communicated to the Whistleblower without delay, unless the Whistleblower has opted out or the communication is anonymous, and to all other interested parties.

3.8.9. Communication

The Reporting Committee cooperates with the relevant corporate functions (e.g. management, compliance functions, human resources, public relations, etc.) to define who is competent to communicate with the various relevant stakeholders, and to effectively plan the manner and content of such communications.

The Reporting Committee plans communication with governmental authorities on the specific issues under investigation, if applicable.

Before communicating with them, corporate legal counsel (internal or external) and any existing guidelines should be consulted to ensure that the interests and rights of the organisation are fully protected.

4. RETENTION

The Company will keep a record of all Reports received.

The Reporting Register is not public, therefore the records and data it contains will be kept confidential.

Records will not be kept longer than necessary and, in any case, for as long as necessary to comply with any applicable legal requirements at any given time.

Reports of irregularities or other cases that do not qualify as Violations included in this Procedure shall be deleted, unless an obligation to further retain them arises from other Procedures in force at the Company, in which case they will be processed within the limits provided for by the same.

Once the investigation of the Report has been concluded and the appropriate actions have been taken, as the case may be, the data of the Report that has been followed up will be duly blocked-in order to comply with the legal obligations that may be applicable in each case.

In no case may the data (report, related documentation) be kept for a period longer than **5 years from the date of the documentation of the final outcome** of the reporting procedure.

If it is decided not to follow up the Report submitted, the information may be kept anonymously.

The aforementioned term of five years is without prejudice to the different term provided, on the other hand, for the preservation of data, deeds and documents relating to the proceedings (e.g. disciplinary proceedings) initiated and to the initiatives (e.g. corrective measures, compensation, etc.) taken by the Company in total or partial dependence on the Report.

In Austria

Report documentation must be deleted 5 years after the last processing or transmission of data, a period that may be extended for the purposes of ongoing proceedings (administrative, judicial or criminal).

Access logs: 3 years after that date of termination. Example: if the report data is deleted after 5 years (2030), the related access logs remain available until 2033 for any ex post checks on data breaches or abuses.

In Germany

Report documentation must be deleted 3 years after the conclusion of the proceedings, except for necessary and proportionate extensions to comply with other legal obligations (e.g. HGB, AO) or to defend against claims.

5. LEGAL PROTECTION

The Whistleblower and the other Protected Subjects are guaranteed by the Companies the Protections indicated in ***Appendix B***.

6. TRAINING

The training, communication and information activities represent an indispensable component for the effective implementation of the Whistleblowing management and are regulated in ***Appendix D***.

7. DISTRIBUTION

The Whistleblowing Managers shall make available to the Addressees of this Procedure, clear information on the Reporting Channels, on the prerequisites for making internal and external Whistleblowing Reports and Public Disclosures, and on the Safeguards available to the Protected Subjects using one or more of the following methods:

- Posting in a visible place in the workplace (Company notice board),
- Making available
 - ✓ by hand and/or
 - ✓ via e-mail, or
 - ✓ via the Company intranet or
 - ✓ via another software application (e.g. personnel and/or payslip management software or procedure distribution software),
- Publication in a specific section of the corporate website (the URL address of which is communicated by the Company),
- Made available through a link/icon on the first electronic page of the Report Portal/Software.

8. **SANCTIONS**

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

Furthermore, the Company expressly reserves the right to penalise those who are found to be responsible for the aforementioned offences.

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

Italy

Whoever:

- obstructs or attempts to obstruct a Whistleblower or the other Protected Persons. in connection with any Reporting, or puts them under pressure through intentional 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 ANAC - the National Anti-Corruption Authority, with an **administrative fine** ranging from EUR 10,000.00 to EUR 50,000.00.

Austria

Whoever:

- obstructs or attempts to obstruct one of the Whistleblowers or the other Protected Persons. in connection with any Whistleblowing 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 event of a repeat offence up to EUR 40,000.00.

Germany

Anyone who

- obstructs a Whistleblower or other Protected Persons in relation to a Report,

- fails to establish or maintain an Internal Reporting Channel despite being obliged to do so,
- takes retaliatory measures or,
- intentionally or negligently fails to maintain confidentiality,

commits an administrative offence, punishable by a fine of up to €500,000.00, depending on the offence.

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, D.Lgs. 24/2023 (Whistleblowing Decree), and the further regulations referred to therein;
- in relation to reports concerning the Company SALVAGNINI MASCHINENBAU GMBH, the Whistleblowers Protection Act (HSchG), and the further regulations referred to therein.
- in relation to reports concerning SALVAGNINI Deutschland GmbH, the Whistleblower Protection Act (HinSchG) and other regulations mentioned therein.

10. CHANGES

This Procedure may be amended or updated, at any time, in accordance with operational, legislative or regulatory requirements and based on lessons learned during its actual application. Such amendments shall be promptly communicated to all persons involved and shall become binding from the moment of their communication or, if necessary, from the effective date established by the Company.

If the changes are substantial, they shall be approved by the competent bodies of the Company.

APPENDIX A - SECTORAL VIOLATIONS

Sectoral Violations include:

- a) **offences** (acts and omissions, even if only attempted or concealed) **that fall within the scope of the following sectoral acts of the Union**⁸:

Protection of Privacy and Protection of Personal Data

Examples

- Omitted or inaccurate privacy notices to employees, applicants, visitors, customers, potential customers, suppliers, agents
- Omitted or inaccurate privacy policy on the corporate website (so-called privacy policy) and/or cookie policy
- Omitted or inaccurate privacy policy on whistleblowing
- Absence or inaccurate privacy policy on video surveillance or automated monitoring and decision-making systems
- Failure to obtain the prior specific consent of the data subject in cases provided for by law
(in particular:
 - ✓ use of the employee's image for advertising purposes
 - ✓ use of the image of guests at company events for advertising purposes
 - ✓ processing of personal data for direct marketing, profiling or market research purposes)
- Failure to obtain a trade union agreement or administrative authorisation for video-surveillance or automated monitoring and decision-making systems
- Failure or deficiency of register of processing operations
- Failure or deficiency of appointment of external data controllers
- Failure or deficiency of co-ownership agreements for processing in cases required by law
- Failure to distribute written appointments and instructions to employees on the processing of personal data
- Failure to comply with the privacy clauses of the corporate Whistleblowing Procedure
- Failure to adopt organisational (e.g. physical, managerial) or technical (in particular, IT) protection measures suitable to avoid/reduce the risk of unauthorised access, loss or alteration, even accidental, of personal data processed by the company
- Failure to draw up a DPIA (assessment of the impact of a given processing operation or set of processing operations on the rights of data subjects) in the mandatory cases provided for by law
- Failure or delay in handling requests received by the company to exercise data subjects' rights

Protection of the environment

⁸ See Annex to EU Directive 1937/2019.

E.g. so-called environmental offences, such as the discharge, emission or other release of hazardous materials into the air, soil or water or the unlawful collection, transport, recovery and disposal of hazardous waste.

E.g. violations of administrative requirements punished by administrative fines.

Product safety and conformity

E.g. Violations of obligations aimed at ensuring that any product manufactured or marketed by the Company [...], under normal or reasonably foreseeable conditions of use, including duration and, where appropriate, commissioning, installation and maintenance, does not present any risk or only minimal risks, compatible with the use of the product and considered acceptable in compliance with a high level of protection of the health and safety of persons [...].

E.g. Infringement of the producer's obligation to provide the consumer with all information relevant to the assessment and prevention of risks arising from normal or reasonably foreseeable use of the product.

E.g. Infringement of the producer's obligation to take measures proportionate to the characteristics of the product supplied to enable the consumer to be informed of the risks.

NB: A product is defective when it does not offer the safety that may legitimately be expected taking into account all the circumstances, including:

(a) the manner in which the product was put into circulation, its presentation, its obvious characteristics, and the instructions and warnings provided;

(b) the use for which the product may reasonably be intended and the behaviour which may reasonably be expected in connection therewith; the time during which the product was put into circulation.

A product is defective if it does not offer the safety normally offered by the others in the same series.

N.B. The scope of risk relevant here goes beyond the mere presence of product flaws and defects (e.g. damage, failure to function, aesthetic appearance not corresponding to the agreed description, etc.) which, however, do not translate into a real **safety risk** for the purchaser/user even though they affect suitability for use or the promised qualities.

Anti-money laundering and terrorist financing

The offence of money laundering exists when, apart from cases of complicity in the offence, a person replaces or transfers money, goods or other utilities originating from a crime, or carries out other transactions in connection with them, in such a way as to obstruct the identification of their criminal origin.

The offence of financing terrorism exists when any person (i) collects, disburses or makes available property or money intended to be used, in whole or in part, for acts of terrorism, or (ii) deposits or keeps property or money intended for such purposes (even if not subsequently used).

(only in Austria)

Prevention and Punishment of Offences under Sections 302-309 of the Austrian Criminal Code (StGB), Federal Law Gazette No. 60/1974:

- Art. 302 Abuse of Office
- Article 303 Unlawful restraint or deprivation of liberty and Unauthorised search of a dwelling
- art. 304 Corruption in public acts
- Article 305 Acceptance of benefits
- Article 306 Acceptance of benefits to influence
- Article 307 Passive corruption
- Article 307a Granting of benefits
- Article 307b Granting of benefits to influence
- Article 308 Undue influence in public acts
- Article 309 Corruption in private acts

(only in Germany)

- Violations punishable by law,
- violations subject to financial penalties if the violated regulation serves to protect life, physical integrity or health or to safeguard the rights of employees or their representative bodies.
- violations of regulations on the safe transport of dangerous goods by road, rail and inland waterways,
- violations of requirements to promote the use of energy from renewable sources and energy efficiency,
- breaches of rules on quality and safety standards for organs and substances of human origin, medicinal products for human and veterinary use, medical devices and cross-border healthcare,
- breaches of regulations on the manufacture, presentation and sale of tobacco products and related products,
- breaches of provisions governing the rights of shareholders in public limited companies,
- violations of accounting and auditing obligations for public interest entities within the meaning of section 316a(2) of the German Commercial Code (HGB),
- breaches of tax regulations,
- violations of competition protection rules,
- statements by public officials that constitute a breach of the obligation to uphold the Constitution.

b) **acts or omissions detrimental to the Union's financial interests** referred to in Article 325 TFEU specified in the relevant EU secondary legislation;

According to Article 2 of the relevant Directive, 'financial interests' includes all revenue and expenditure covered by the Union budget, including VAT revenue.

Examples of infringements: fraud involving Community resources; cross-border VAT fraud; Violations of customs law.

- c) **acts or omissions relating to the internal market**, as referred to in Article 26(2) TFEU, including:
- a. violations of Union competition rules (e.g. abuse of dominant position, agreements between companies restricting competition in the internal market, merger rules)
(N.B.: these regulations do not apply to the companies to which this Procedure is addressed and are therefore relevant only in the event that the companies, in their capacity as suppliers and/or partners of third parties, detect possible violations in this matter exclusively referable to the activity of the latter)
 - b. Violations of the Union rules on **State aid**
(e.g. falsification of data and information in order to obtain state aid that is not due, use of state aid for purposes other than those for which it was granted, false reporting)
 - c. internal market violations related to acts in breach of **corporate tax** rules
(e.g. any accounting/tax irregularity aimed at distorting the correct assessment of IRES, IRAP, such as under-declaration of turnover, over-declaration of costs, invoicing of nonexistent transactions, deduction of non-deductible costs, creation and use of slush funds), or
 - d. **practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the applicable corporate tax law.**
- d) **Acts or omissions that frustrate the object or purpose of the provisions of Union acts** in the areas indicated in points (a), (b) and (c).

E.g. abusive practices as defined by the case law of the EU Court of Justice. Consider, for example, an undertaking operating on the market in a dominant position: the law prevents such an undertaking from acquiring, on the basis of its own merits and abilities, a dominant position on a market, or from ensuring that less efficient competitors remain on the market. However, such an undertaking could jeopardise, by its own conduct, effective and fair competition in the internal market by resorting to so-called abusive practices (adoption of so-called predatory pricing, target rebates, tying) in Violations of the protection of free competition.

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

APPENDIX B - PROTECTIONS

1. PROTECTED PERSONS

The Protected Persons include,

- the Whistleblower (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 lodging a complaint with the judicial authority or the person making a Public Disclosure and who are related to them by a stable emotional or kinship relationship up to the fourth degree (cousins),
 - **Co-workers** of the Whistleblower, of the person who has filed a judicial report or made a Public Disclosure, who work in the same employment context as the Whistleblower and who have a usual and current relationship with the Whistleblower,
 - **Entities that own, or are employers of, or operate in the same work environment as the aforementioned persons.**

In Austria

Subjective scope of application of the Austrian HSchG (§ 2)

Person(s) who have obtained information about legal violations due to a current or previous professional relationship with a legal entity in the private sector (§ 5 no. 11) or public sector (§ 5 no. 10):

- **as employees or collaborators of the legal entity,** or as temporary workers at that entity, or
- as **job applicants,** trainees or interns at the legal entity, or as other persons undergoing training at the legal entity, or
- **as self-employed persons,** or
- **as members of an administrative, management or supervisory body of the legal entity,** or
- **carrying out activities under the supervision and direction of a contractor, subcontractor or sub-subcontractor of the legal entity or its suppliers,** who work or have worked in this context.

The HSchG also applies to **shareholders** of legal entities who have obtained information about legal violations due to current or previous professional relationships with such entities.

The provisions of **Sections 4 and 5 of the HSchG** also apply:

- to **natural persons who assist whistleblowers** in the reporting process,
- to **natural persons close to the** who, although not supporting the report, may suffer negative consequences as a result of it, such as retaliation,

- **legal entities wholly or partially owned by the** , or for which the Whistleblower works or with which he or she has a professional relationship.

In Germany

Whistleblowers within the meaning of the HinschG are natural persons who have obtained information about illegalities in connection with their professional activities. These whistleblowers include, in particular:

- Employees,
- persons employed for their professional training,
- civil servants,
- judges, with the exception of honorary judges,
- military personnel,
- persons who are to be regarded as workers assimilated to employees because of their economic dependence; this also includes persons working from home and persons treated as such,
- persons with disabilities employed in a workshop for persons with disabilities or by another service provider within the meaning of Section 60 of Book IX of the German Social Code.

2. PROTECTIONS

In the event of a Whistleblowing, the following three categories of legal protections are guaranteed to **all Protected Persons**:

- PROTECTION MEASURES,
- SUPPORT MEASURES,
- RIGHT TO CONFIDENTIALITY,

as set out below.

With regard, moreover, to the **Whistleblowers only**, the Safeguards also apply when the Report or the complaint to the judicial authority or the Public Disclosure occurs in the following cases

- when the legal relationship** with the Companies **has not yet started**, if the information on the Violations has been acquired during the selection process or in other pre-contractual phases
- during the probationary period**
- 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 the Safeguards.

3. PROTECTIVE MEASURES⁹

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

- Prohibition of Retaliation,
- Protection from Retaliation,

⁹ The protection provided for the Whistleblower will only be guaranteed in the case of reports made by clearly identified persons. The disclosure of the identity by the Whistleblower may take place at any time even after the Report, without prejudice to the protection granted above.

- Limitations of Liability,
- Waivers and Conditional Settlements.

NB: The Protection Measures also apply:

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

(b) in cases of External Reports 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 Reports 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 Reporting or Whistleblowing or Public Disclosure and which causes or may cause the Whistleblower, directly or indirectly, unjust damage*) (**prohibition of retaliatory acts**).

“Retaliation” is to be **understood extensively**, 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 on access to it;
- (e) **demerits or negative references**;
- f) the adoption of **disciplinary measures** or any other sanction, including a fine;
- (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) the **non-renewal** or **early termination** of a fixed-term employment contract
- (k) **damage**, including to a person's reputation, in particular on social media, or **economic or financial** loss, including loss of economic opportunities and loss of income;
- l) inclusion on improper lists (e.g. **blacklists**) on the basis of a formal or informal sector 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 a contract for the supply of goods or services; the introduction of detrimental changes** to the service or supply contract;
- n) the **cancellation of a licence or permit**;
- (o) the request to undergo **psychiatric or medical examinations**.

3.2. Protection from Retaliation

3.2.1 Retaliation

In the event that a member of the Company, in contravention of the provisions of this Procedure, engages in direct or indirect retaliatory acts, the Company itself shall take the necessary measures to ensure that such acts cease as soon as possible and, where appropriate, shall take the necessary disciplinary or liability measures against those responsible.

3.2.2 Reporting to the Public Authority

In Italy

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

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

In Austria

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

3.2.3 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 Subject may invoke, even cumulatively:

- The **nullity *ex lege* of the acts of Retaliation**, which follows the restoration of the situation prior to the same.
- **Reinstatement in** the workplace in accordance with the legislation applicable to the employee, if the Protected Subject has been dismissed because of the Report.

In Austria

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

- restore the *status quo ante*,
- compensate the unlawful act and
- pay damages suffered by the Whistleblower.

In Germany

In the event of a violation of the prohibition of retaliation, the offender is required to compensate the whistleblower for the damage caused, **including future damages such as loss of salary or professional opportunities. However, immaterial damages such as moral pain are not included, unless other civil law provisions apply (e.g. § 253 BGB).**

The violation does not **give rise to any right to establish an employment relationship, vocational training or other contract, nor to professional promotions.**

3.2.4 Burden of Proof

In Italy

In the context of lawsuit or administrative proceedings or, in any case, of ADR disputes concerning the ascertainment of conduct, acts or omissions, constituting prohibited retaliation, it is presumed that the same have been put in place on account of the Report or Public Disclosure.

The burden of proving that they are motivated by reasons unrelated to the Report or Public Disclosure shall be on the person who has committed them.

In the event of a **claim for damages filed by the Whistleblower** (not, therefore, also by other Protected Persons), if he proves that he has made a Report or Public Disclosure (according Whistleblowing Decree) and has suffered damage, **it is presumed, unless proven otherwise, that the damage is a consequence of such Report or Public Disclosure.**

In Austria

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

In lawsuit 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, after assessing all the circumstances, it is more likely than not that another motive was decisive for the act. The link between the act and the Report shall therefore be reasonably proven by the Whistleblower.

In Germany

If a Whistleblower suffers a disadvantage in relation to their professional activity and claims that they suffered it as a result of a Report or disclosure under this law, it is presumed that such disadvantage is retaliation for that Report or disclosure.

In such a case, the person who penalised the whistleblower must prove that the penalty was based on sufficiently justified grounds or that it was not based on the report or disclosure.

3.3. Limitations of liability

The reporting entity or person is not criminally liable, and any further civil or administrative liability is also excluded, for the disclosure or dissemination of Breach Information:

- violations covered by **secrecy** obligations (official, corporate, professional, scientific, commercial or industrial) (punishable by Articles 326, 622, 623 of the Criminal Code),
- violations relating to copyright protection,
- violations relating **to the protection of personal data** (privacy),
- violations offending the reputation of the Involved Person,

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 Reporting, Public Disclosure or the reporting to the judicial authorities.

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

- a) if the Whistleblower commits an **offence in order to acquire or access the Information** that is the Involved Person.

E.g. the offence of unauthorised access to a computer system exists in relation to the act of a person who has intentionally hacked into the e-mail system of a work colleague in order to obtain evidence in support of the Report, and

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

The Companies may also order the imposition of **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).

In Austria

§ 22 HSchG

(1) Whistleblowers who deserve protection under § 6(1) and persons in their entourage (§ 2(3)) **shall not be liable** for the material or legal consequences of a well-founded report.

(2) A report made in accordance with the provisions of **Section 2** (Procedure for internal reports) and a report made in accordance with the provisions of **Section 3** (Procedure for external reports) which reveals facts or information that the whistleblower is required to keep confidential under a legal provision or contractual agreement **does not constitute a breach of confidentiality obligations**, provided that:

1. The report, within the meaning of paragraph 1, **is justified** and, in particular, does not fall under the cases referred to in § 3 paragraph 6, nos. 1–5.

§ 3 Abs. 6 excludes the following five priority cases from the protection of § 22) for reasons of national security:

Nos. 1: public safety and public order;

Nos. 2: national defence and military security;

Nos. 3: state security (e.g. intelligence);

Nos. 4: matters covered by state secrecy or classified information (§ 3 Z 39 BVergG 2012 or Informationssicherheitsverordnung);

No. 5: ongoing judicial investigations or criminal proceedings.

If the report concerns one of these areas, it is not 'justified' for the purposes of § 22 and the whistleblower remains liable to ordinary penalties (e.g. § 122 StGB for breach of company secrets).

2. The whistleblower has **sufficient grounds to believe** that the information is necessary to identify or prevent a violation of the law.

In Germany

A Whistleblower **cannot be held legally liable** for obtaining or accessing information that they have reported or disclosed, provided that such obtaining or accessing **does not in itself constitute a separate offence**.

A Whistleblower does **not violate confidentiality obligations** and cannot be held legally liable for the disclosure of information made in the context of a report or disclosure, if they have **reasonable grounds to believe** that the disclosure was necessary to bring an offence to light.

3.4. Prohibition of Transaction (Italy only)

The rights and protections provided in favour of the Whistleblower **may not be subject to waiver or settlement, in whole or in part**, which, therefore, shall be deemed invalid, unless made in the form and manner provided for by Article 2113, fourth paragraph, of the Civil Code.

4. SUPPORT MEASURES

In Italy

The Whistleblower is entitled to **support measures** consisting of **free information, assistance and advice** on the modalities of Whistleblowing and on the protection from retaliation offered by national and European Union legislation, on the rights of the Involved Person, as well as 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 Third Sector Entities is published on the website: <https://www.anticorruzione.it/-/whistleblowing>.

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

In addition, the Whistleblower 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 SALVAGNINI MASCHINENBAU GMBH , the Reporting Parties and other Protected Subjects are entitled to legal aid in criminal and civil proceedings, provided they are entitled to legal aid in accordance with the provisions of the Austrian 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 Involved Person, 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 up on them.

The non-anonymous Whistleblower shall be guaranteed confidentiality by the Companies, the Case Managers and anyone else involved in the receipt and processing of a Report:

- **his/her identity and that of the persons close to him/her facilitating** the Report (right to anonymity), throughout the entire Reporting process, to anyone who is not the Case Manager¹⁰, and
- **the content of the Report**, including the **documentation** attached to it, to the extent that its disclosure, even indirectly, may allow the identification of the Whistleblower.

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

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

5.2. Exclusion of confidentiality

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 in order to safeguard the rights of defence of the person reported.

To this end, the **Involved Person should be warned without delay by the Case Managers of an unsubstantiated Report made in bad faith or with gross negligence against him/her** in order to be able to consider whether to exercise any rights against the person making the Report¹¹; or

ii) the existence of an obligation to communicate the name of the Whistleblower to **Courts or law enforcement authorities**, or

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

(iv) if knowledge of the identity of the Whistleblower is indispensable for **the accused person's defence**, only in the presence of the Whistleblower's express consent to the disclosure of his/her identity.

¹⁰ Confidentiality also covers all other information from which the identity of the Whistleblowers can be deduced directly or indirectly.

¹¹ 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 ascertained 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 can 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 shall be ensured where he is not in bad faith; in fact, the purpose of 'whistleblowing' could be frustrated if it were expressly provided that the Whistleblower shall be informed of an unfounded report but not in bad faith, especially in the case of minor negligence (not punishable even at disciplinary level, but theoretically - although it is rare - prosecutable in civil proceedings).

In any case, the Whistleblower **shall be informed in writing** by the Case Managers 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 proceedings¹².

The Companies, the Case Managers and anyone else involved in the receipt and processing of a Report shall also protect **the identity of the Involved Person and of the other persons mentioned in the Report** until the conclusion of the proceedings initiated as a result of the Report, in compliance with the same guarantees of confidentiality provided for in favour of the Whistleblower.

In Austria

The identity of Whistleblowers and any person concerned by the report may **only** be disclosed if an administrative authority, court or public prosecutor's office deems such disclosure to be **indispensable** in administrative or judicial proceedings, or in investigative proceedings under the Austrian Code of Criminal Procedure, **and** if such disclosure is considered **proportionate** to any risk to the whistleblower, in light of the validity and seriousness of the allegations made.

In Germany

The identity of a Whistleblower who **intentionally or through gross negligence** provides incorrect information about offences **is not protected** under the HinSchG.

Information about the identity of the Whistleblower or other circumstances that allow their identity to be traced may be forwarded to the competent authority:

- by internal reporting offices, to other competent bodies (internal or external) if this is necessary in the context of internal investigations at the employer or in the organisational unit involved,
- **in criminal proceedings**, at the request of the investigating authorities,
- on the basis of a measure adopted in administrative proceedings following a report, including administrative penalty proceedings,
- **pursuant to a decision by the judicial authority**,
- by **the Federal Financial Supervisory Authority (BaFin)**, in its capacity as an external reporting office pursuant to Section 21, to the competent specialist departments within BaFin and, in the case of transactions referred to in Section 109a of the German Securities Trading Act (Wertpapierhandelsgesetz), to the bodies specified therein, or
- by the Federal Cartel Office (**Bundeskartellamt**), as an external reporting office within the meaning of Section 22, to the relevant specialist departments within the Bundeskartellamt and, in the cases provided for in Section 49 (2) second sentence and (4) and Section 50d of the Act against Restraints of Competition, to the respective competent competition authority.

Furthermore, information relating to the identity of the whistleblower or other circumstances that allow them to be identified may **only** be disclosed **if disclosure is necessary for follow-up measures** and the whistleblower has **given their prior consent** to disclosure.

6. PREREQUISITES OF THE PROTECTIONS. UNFOUNDED, BAD FAITH OR GROSSLY NEGLIGENT REPORTING

The Safeguards apply if the following **conditions** are met:

¹² The competent authority, when informing the Whistleblower, sends the Whistleblower a written explanation of the reasons for disclosing the confidential data in question.

- a) at the time of the Report or Public Disclosure, the Whistleblower had **reasonable grounds to believe that the Violations Information** 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 the Protected Subjects also exists in the case of **Reports or Disclosures that later turn out to be unfounded**, if the Whistleblower, at the time of the Report or Public Disclosure, 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 fell within the scope of this procedure.

Safeguards in favour of the Protected Subjects are not guaranteed, and a disciplinary sanction shall also be imposed on the Whistleblower, if **it is established, even by a first instance judgement:**

- i) **criminal liability** of the Whistleblower for offences of slander or defamation in relation to the facts reported, or
- ii) **the civil liability** of the Whistleblower, 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 with the **awareness of the abuse/instrumentalisation** of the Reporting procedure, e.g. manifestly unfounded, **opportunistic** and/or made for **the sole purpose of damaging** the Reported Person or other persons mentioned in the Report (employees, members of corporate bodies, suppliers, partners, group companies, etc.) are to be considered in **bad faith/gross negligence** (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 set out in Chapter 3.3.2.2 of the Procedure is also met.

In Austria

Whistleblowers and persons associated with them (§ 2 par. 3) **are not liable** for the material or legal consequences of a well-founded report.

In the case of **deliberately false reports**, whistleblowers are liable for any damage caused and are punished with a **fine of up to €20,000** pursuant to § 24 no. 4 HSchG.

In the event of **Public Disclosure**, the Whistleblower benefits from legal protection if, in addition to the basic condition, one of **the Prerequisites for Public Disclosure** set out in Section 3.3.2.2 of the Procedure is also met.

APPENDIX C - PROCESSING OF PERSONAL DATA

1.1 Any processing of personal data carried out for the purposes of the management of the Report shall be carried out in accordance with the legislation on the protection of personal data (GDPR, Supervisory Authority Measures, D.Lgs. 196/2003)¹³.

Consequently, anyone involved in the receipt and processing of non-anonymous Reports **is required to comply with all the procedures, protocols and written security instructions provided for by the Company's privacy system**, without prejudice to the further rules set out in this procedure.

It is understood that the Companies' **Privacy Notice on Whistleblowing** is to be considered as a procedure, containing specific data processing rules whose compliance by the Companies is essential to ensure the compliance of the 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 accidentally received or collected, shall be promptly deleted** by the relevant Case Manager with respect to the Breach.

1.3 The above processing operations shall be carried out by the Company (data controller) **in compliance with the general principles set out in Articles 5¹⁴ and 25¹⁵ GDPR**, as well as by taking appropriate measures to protect the rights and freedoms of the data subjects.

¹³ And, 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.

¹⁴ Art. 5 GDPR: Personal data shall be:

- (a) processed lawfully, fairly and transparently towards the data subject ("lawfulness, fairness and transparency");
- (b) collected for **specified, explicit and legitimate purposes**, and further 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**; every reasonable step shall be taken to ensure that data which are inaccurate in relation to the purposes for which they are processed ('accuracy') are erased or rectified without delay
- (e) **kept** in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which** they are processed ('limited storage'); and
- (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')

¹⁵ Article 25 GDPR: Article 25 Data protection by design and data protection by default

1. Taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, as well as risks of varying likelihood and severity to the rights and freedoms of natural persons constituted by the processing 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 processing are processed by default. This obligation

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

- defines, by means of this procedure and its annexes, the model for receiving and managing Internal Reports, identifying appropriate technical and organisational measures to guarantee a level of security appropriate to the specific risks arising from the processing operations performed,
- provides for the execution of the Data Protection Impact Assessment (DPIA) carried out by the Privacy Function itself, and
- regulates the relationship with any external suppliers that process personal data on behalf of the Company(s) pursuant to Article 28 GDPR (appointments of external Data Processors, e.g., external Case Manager(s) designated by the Company, third-party Portal/Software Managers);
- shall provide, and/or identify the different corporate Functions in charge of providing, suitable **information** to the Whistleblower, to the Involved Person and to the other relevant categories of **data** subjects, suitable **notice on the processing of personal data** (pursuant to Articles 13 and 14 GDPR), in compliance with the texts approved by the competent Board of Directors of the Company.

1.5 The Case Managers shall ensure that the Internal Reporting Channels other than the "Portal/Software" are implemented and managed in a secure manner and such as to guarantee the confidentiality of the identity of the Whistleblower and of any third parties mentioned 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 **the EQS Portal Software Manual ver. 3 (Appendix E)**.

The configuration of the basic functionalities of the Portal/Software is the responsibility of the designated Admin role(s), while the 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 the SALVAGNINI Group, aimed at:

- i) regulate the **sharing of resources** (e.g. Portal/Software) for the receipt and management of Whistleblowing Reports and,
- ii) determine the respective **responsibilities** regarding compliance with personal data protection obligations, pursuant to Article 26 GDPR, as follows:
 - **Privacy role:** each Company acts as co-processor with respect to the processing of data related to:

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.

- **the sharing of the Internal Reporting Channel** consisting of the SaaS Integrity Line Portal/Software; and
- **the Whistleblowing Policy** for the communication/collection and processing of Reports.
- **Notice to data subjects pursuant to Article 13 GDPR:**
 - a) the privacy notice to Whistleblowers is made available to the data subject by the competent Case Managers, as follows:
 - ✓ by means of a link/text that can be viewed on the landing page, if the Whistleblower (also anonymous) **uses the Portal/Software** to send the Report
 - ✓ by hand delivery, at the first useful opportunity, in case of **personal meeting** with the Whistleblower not preceded by the use of the Portal/Software to send the Report;
 - ✓ in the event that the Whistleblower **calls** the Company to make the Report: by means of verbal notice to the Whistleblower about the availability of the Report on the Portal/Software
 - ✓ by means of a specific document/link/viewable hypertext made available in the Secure Inbox, if the **Report is anonymous** and reaches the Company by an **offline** means (e.g. by registered letter with advice of delivery) and is then **entered autonomously in the Portal/software by the person receiving the Report;**
 - b) the privacy notice to the Subjects of the Report (natural persons to whom the reported Breach is charged) is made available to the data subject by the Case Managers, in the following ways
 - ✓ by hand delivery, at the first useful opportunity, in the event of a **personal meeting** with the Involved Person;
 - ✓ by means of a link/text viewable on the landing page, if the Involved Person **uses the Portal/Software** to interact with those assessing the Report;
 - ✓ if the contact with the Involved Person takes place by **telephone**: by means of verbal notice to the data subject about the availability of the 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 managing the exercise of the data subject's rights, to which reference is made herein;
- **personal data breaches:** each Company acts as an autonomous data controller in accordance with its own data breach management procedures, to which reference is made herein;
- **security measures:** each Company of the Group is required to comply with the security measures provided for i) by this Procedure, ii) by the functional specifications of the Portal/Software, ii) by its own privacy system, iv) by the personal data protection legislation applicable to it;
- **operational interface with the third party supplier of the Portal/Software:** the Parent Company acts as centralised technical interface towards the supplier, on behalf of the other Companies, on the basis of a mandate with representation to be understood as conferred herein.

APPENDIX D - TRAINING

Training of Case Managers

Specific training, to be periodically updated, should be addressed, first and foremost, to the people in charge of or involved in the Whistleblowing management process, with the aim of providing them with the fundamental skills needed in the implementation and effective management of the whistleblowing processes, as well as the knowledge of the issues covered by the reports (see ANAC Guidelines, point 5).

These people should receive detailed training on the different facets related to the management of whistleblowing in order to promote their autonomous and ethical, as well as professional, operation. Therefore, staff should be trained on at least the following topics

- the regulatory profiles of whistleblowing (both the European legislation and the provisions contained in D.Lgs. 24/2023), with particular attention also to the issue of personal data protection, in order to ensure maximum security and confidentiality of information
- the procedures and operating methods, with specific focus on the requirements to be fulfilled by Whistleblowers, including the management of conflicts of interest;
- the general principles of conduct (confidentiality and privacy, ethics and integrity, active listening, communication skills and cooperation).

As an alternative to the aforementioned training, the aforementioned specific skills and knowledge may be appropriately demonstrated by the Whistleblowers by means of CVs, certificates or similar documentation to be provided to the relevant HR function.

Training for all employees and non-employees of the entity

The training should involve all the employees and collaborators of the Company, so as to provide a clear and exhaustive picture of the new rules (clarifying, for instance, who the Whistleblower is, what can be reported and through which channels, what protections the law guarantees to the Whistleblower and which reports, on the other hand, do not fall within those protected, as well as specifying the involvement - also guaranteed by the protections - of the various persons working in the same work context as the Whistleblower).

The HR Function, in agreement with the person in charge 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

- *EQS Portal Software Manual ver. 3*