GRUPPO DE ECCHER

WHISTLEBLOWING PROCEDURE

REV.	DATE	PREPARED	CONTROLLED	APPROVED
12	07.05.2025	Avvera Consultant for 231 Model	L. Cogorno QHSE Director	E. Barbiero CEO

Luigi Cogorno
Digitally signed by Luigi Cogorno
DN: C=IT, OU=C-QHSE, O=QHSE, CN=Luigi Cogorno, E=l.cogorno@rde.it
Reason: I am the author of this document
Location: your signing location here
Date: 2025.05.23 16:07:12+02'00'
Foxit PDF Editor Version: 11.0.0

Firmato digitalmente da:
Barbiero Enrico
Firmato il 23/05/2025 15:29
Seriale Certificato: 3238295
Valido dal 26/01/2024 al 26/01/2027
InfoCamere Qualified Electronic Signature CA

REV.	DATE	DESCRIPTION OF THE REV	PREPARED	CONTROLLED	APPROVED
12	07.05.2025	Internal report channel update	Avvera Consultant for 231 Model	L. Cogorno QHSE Director	E. Barbiero CEO
11	16.09.2024	Model 231 update			
10	14.07.2023	Regulatory update (D.lgs. 24/23)			
01	01/01/2021	Model 231 update			
00	7/ 12/ 2018	First issue			

INDEX

SCOPE 4
AREA OF APPLICATION 4
GENERAL PRINCIPLES 4
ABBREVIATIONS AND ACRONYMS 5
REFERENCE DOCUMENTS 5
INTERNAL DOCUMENTS 5
DEFINITIONS 6
WHISTLEBLOWING PROCEDURE 11
THE REPORTS COVERED BY THIS PROCEDURE 11
SCOPE OF APPLICATION 12
COMPANY PERIMETER 12
REPORTING MANAGEMENT PROCESS 12
INTERNAL SIGNALLING THROUGH OTHER CHANNELS 13
HANDLING OF REPORTS OF VIOLATIONS PURSUANT TO LEGISLATIVE DECREE 24/23 16
INTERNAL REPORTING 16
RECEPTION AND ANALYSIS OF INTERNAL REPORTING 16
PENALTY SYSTEM AND DISCIPLINARY 18
PROTECTING THE REPORTING PERSON AND ENFORCING PROTECTION MEASURES 19
LIMITATIONS OF LIABILITY 20
STORAGE AND ARCHIVING 21
REPORTING 21
SPECIAL CASES 21
RESOLUTIONS OF THE SUPERVISORY BOARD 21
AND RESPONSIBILITIES 21
DISTRIBUTION AND STORAGE 22

SCOPE

The purpose of this procedure is to regulate the process of handling Reports of Violations pursuant to Legislative Decree 24/23, in a manner that guarantees the protection of the identity of the Reporting Person, and reports concerning the risks of corruptive phenomena, as referred to in the management system for the prevention of corruption (ISO 37001:2016), reports concerning issues covered by SA8000 certification (working conditions, sustainable development, social issues, etc.) and reports concerning issues covered by PdR125 certification (e.g. accidents, reports of violence or abuse, performance indicators [Key performance indicators] not in line, etc.).
With this procedure, the Company defines its model for the receipt and management of internal reports, as well as the internal reporting channel, identifying technical and organizational measures suitable for guaranteeing a level of security appropriate to the specific risks arising also from the processing of personal data carried out to manage them, in compliance with the provisions of Regulation (EU) 2016/679 and Article 18 of Legislative Decree No. 51 of 2018.

AREA OF APPLICATION

The procedure applies to the Rizzani De Eccher Group (hereinafter RdE) and to Rizzani de Eccher SpA. As regards the other companies of the RdE Group (be they subsidiaries, affiliates, special purpose companies or other legal forms) this procedure can be carried out own by each individual Company, approved by its decision-making body and become part of the procedural body of the same. Where other companies in the group do not wish to fully adopt the text of this procedure, they are required to adapt their procedures using this procedure as a guideline within which to move. In the event that the governing body of the individual companies wishes to go outside the Guidelines outlined in this procedure, it will not have to immediately inform the person responsible for this document for the appropriate assessments. The implementation of this procedure or its modifications for subsidiary companies must take place within 90 days of its issuance through the resolution of the Board of Directors (BoD).

GENERAL PRINCIPLES

People involved in the activities defined by the Standard Procedure described in this document must operate in compliance with the regulatory, organizational, and power systems. They must also act in accordance with the law, applicable regulations, and adhere to the principles outlined below.

Traceability – The persons involved in this Standard Procedure, within their area of responsibility, must ensure that documentation and related activities concerning the process remain traceable. Additionally, each document must be archived in accordance with regulations, respecting the dedicated information systems provided.

Confidentiality – The persons involved in activities related to this Standard Procedure must ensure an appropriate level of confidentiality regarding the information contained in the document by virtue of their position. Moreover, they are required not to disclose confidential information without the Group's authorization.

Separation of Duties – In the activities governed by this Standard Procedure, the separation of duties and responsibilities must be established to ensure an appropriate distribution of tasks, thereby reducing risks associated with the reliability of information and the correct performance of tasks.

Conflict of Interest – Relationships between personnel involved in activities of this Standard Procedure and their counterparts must aspire to the highest standards of ethical behavior in accordance with the Code of Ethics of Rizzani De Eccher S.p.A. Any situation that leads to a conflict with corporate interests and that might interfere with the impartiality of the personnel's decisions in relation to corporate interests must be avoided, in line with the principles of the Code of Ethics and the Anti-Corruption Policy.

Anti-Corruption Policy – Rizzani De Eccher S.p.A. adopts a strict and absolute prohibition approach towards any form of corruption. Specifically, Rizzani De Eccher S.p.A. prohibits offering, promising, providing, accepting, or requesting an undue advantage of any value (which may be economic or non-economic), directly or indirectly and regardless of the location, in violation of applicable law, as an incentive or reward for a person to act or refrain from acting in relation to the performance of that person's duties. Rizzani De Eccher S.p.A. is committed to adopting and enforcing the Anti-Corruption Management System.

Sustainability – Rizzani De Eccher S.p.A. is committed to implementing a sustainable business model outlined in the Code of Ethics, which identifies a set of principles considered to be priorities, capable of guiding the modus operandi of all stakeholders and generating positive externalities in terms of sustainable development.

Transparency – Individuals involved in activities governed by the Standard Procedure must operate in a manner that ensures maximum transparency, understood as clarity, completeness, and relevance of information, in the performance of their activities, respecting corporate regulations as an implementation of the principle of transparency.

ABBREVIATIONS AND ACRONYMS

The RdE structure provides different levels of organizational management, as identified in the Company Organization Chart, from which the methods of assigning the name of each identified task derive. Within the procedure, each task is referred to by means of an acronym, structured as identified in the operational instruction C-0000-RDE-CMS-IST-01-01 Abbreviations and document coding.

If the procedures are applicable at multiple levels (Corporate, Area or Project) the Functions involved will be referred to using a simplified string composed of the Office acronym.

The following table shows the abbreviations and acronyms used in the procedure:

ABBREVIATIONS AND ACRONYMS	DESCRIPTION
AD	Chief executive officer
HR	Human Resources
PA	Public Administration
Rde	Rizzani de Eccher S.p.A.
SB	Supervisory Body

REFERENCE DOCUMENTS

INTERNAL DOCUMENTS

- REPORT FORM;
- INFORMATION PURSUANT TO ARTICLE 13 OF REGULATION (EU) 679/2016.

DEFINITIONS

The definitions reported below have been defined in line with those defined according to international associations:

NAME	DEFINITION
ANAC	National Anti-Corruption Authority, established by Law No. 190/2012 is the independent administrative authority whose institutional mission is identified as the prevention of corruption in all areas of administrative activity.
Activities at risk of offence	the process, operation, act, or set of operations and acts, which may expose the Company to the risk of sanctions under the Decree on the basis of the commission of an Offence.
CCNL	the National Collective Labour Agreement applicable to the Company's employees and, specifically, the Construction Agreement.
Code of Ethics	the document, officially desired and approved by the Company's top management as an explication of corporate policy, which contains the general principles of conduct - i.e., recommendations, obligations and/or prohibitions - with which the Addressees must comply and whose violation is sanctioned.
Work context	the work or professional activities, present or past, carried out in the context of the relationships referred to in Article 3, paragraphs 3 and 4 of Legislative Decree 24/2023, through which, regardless of the nature of such activities, a person acquires information on violations and in the context of which he/she could risk suffering retaliation in the event of a public disclosure or report to the judicial or accounting authorities.
Legislative Decree 231/2001	or "Decree": Legislative Decree No. 231 of 8 June 2001, containing the "Regulations on the administrative liability of legal entities, companies and associations, including those without legal personality, pursuant to Article 11 of Law No.300" of 29 September 2000, published in the Official Gazette No. 140 of 19 June 2001, as amended and supplemented.
Addressees	Company Bodies (Directors and Auditors)[1], Company Personnel, Suppliers and all those who operate in the interest or to the advantage of the Company, with or without representation and regardless of the nature and type of relationship

[1] This includes any person with functions of administration, management, control, supervision or representation, even if such functions are exercised on a de facto basis.

	with the Principal Company. The Addressees are required to comply with the Model, the Code of Ethics and the Preventive Protocols.
Employees	all natural persons who have an employment relationship with the Company.
Public dissemination	making information about violations publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people.
Facilitator	a person who assists a Reporting Person in the reporting process, operating within the same work context and whose assistance must be kept confidential.
Information on breaches	information, including well-founded suspicions, concerning breaches committed or which, on the basis of concrete elements, could be committed in the organisation with which the reporting person or the person lodging the complaint with the judicial or accounting authority has a legal relationship within the meaning of Article 3(1) and (2) of Legislative Decree 24/2023 (i.e. public sector and private sector) , as well as elements concerning conduct aimed at concealing such breaches.
Guidelines	the Guidelines for the construction of organisation, management and control models pursuant to Legislative Decree 231/2001, published by trade associations, which were considered for the purposes of preparing and adopting the Model.
Organisational, management and control model pursuant to Legislative Decree 231/2001" or "Model"	the Organisational, management and control model deemed by the Corporate Bodies to be suitable for preventing the Offences and, therefore, adopted by the Company, pursuant to Articles 6 and 7 of the Legislative Decree, in order to prevent the Offences from being committed by apical or subordinate Personnel, as described in this document and its annexes.
Corporate Bodies	the Board of Directors and/or the Board of Statutory Auditors of the Company, depending on the meaning of the relevant sentence.
Supervisory Body	the Body provided for in Article 6 of the Legislative Decree, with the task of supervising the operation of and compliance with the organisation, management and control model, as well as its updating.
Personnel	all natural persons who have an employment relationship with the Company, including employees, temporary workers, collaborators,

	"interns", volunteers and freelancers who have been commissioned by the Company.[2]
Key Personnel	the persons referred to in Article 5(1)(a) of the Decree, i.e. the persons who hold functions of representation, administration or management of the Company; in particular, the members of the Board of Directors, the Chairman, the Directors with Delegated Powers, any proxies.
Personnel subject to the direction of others	the persons referred to in Article 5(1)(b) of the Decree, i.e. all Personnel working under the direction or supervision of Senior Personnel.
Reporting person	the natural person who makes a report or public disclosure of information on violations acquired in the context of his/her work context.
Person involved	the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as a person otherwise implicated in the reported or publicly disclosed violation.
Public Administration" or "P.A."	Public Administration is to be understood as: • the State (or State Administration); • Public Entities; it is specified that the Public Entity is either identified as such by law or is an Entity subject to a system of public control, to the interference of the State or other Administration as regards the appointment and dismissal of its directors, as well as the administration of the Entity itself. It is characterised by the participation of the State, or other public administration, in the management costs; or by the power of direction that the State has over its organs; or by institutional public financing; or by the establishment of a public initiative. Purely by way of example and without limitation, the following companies are to be considered Public Administrations in the broadest sense: Ferrovie dello Stato, Autostrade S.p.A., AEM Milano, etc. • Public official: a person who exercises 'a legislative, judicial or administrative public function'. For the purposes of criminal law, 'an administrative function governed by rules of public law and

[2] For the purposes of the "whistleblowing" legislation, the following cases are also considered: when the employment or collaboration relationship has not yet commenced, if information on breaches was acquired during the selection process or in other pre-contractual stages; during the probationary period; after termination of the legal relationship if information on breaches was acquired during the course of the relationship).

	authoritative acts and characterised by the formation and manifestation of the will of the public administration or by its being carried out by means of authoritative or certifying powers' (Article 357 of the criminal code) is public; • Person in Charge of a Public Service: a person who "in any capacity performs a public service. By public service is to be understood an activity governed in the same manner as public function, but characterised by the lack of the powers typical of the latter and with the exclusion of the performance of simple orderly tasks and the performance of merely material work" (Article 358 of the Criminal Code). It should be noted that "in any capacity whatsoever" must be understood as meaning that a person exercises a public function, even without a formal or regular investiture (a "de facto" public service appointee). In fact, the relationship between the P.A. and the person performing the service is not relevant.
Protocol	the organisational, physical and/or logical measure provided for by the Model in order to prevent the risk of commission of the Offences.
Offences" or the "Offence	the set of offences, or the individual offence, referred to in Legislative Decree 231/2001 (as it may be amended and supplemented in the future).
Retaliation	means any conduct, act or omission, even if only attempted or threatened, occurring by reason of the report, judicial or accounting authority report or public disclosure and which causes or is likely to cause the reporting person or the person making the report, directly or indirectly, unjust damage.
Report	the written or oral communication of information on the Violations referred to in Legislative Decree 24/23.
External reporting	the communication, in writing or orally, of information on Violations under LD 24/23, submitted through the external reporting channel.
Internal Reporting	the communication, in writing or orally, of information on Violations under LD 24/23, submitted through the internal reporting channel.
Follow-up"	the action taken by the entity entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigation and any measures taken.

Disciplinary System	the set of sanctioning measures applicable in the event of the Violation being founded.
Company	Rizzani De Eccher S.p.A.
Violations	means conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity and that consist of: 1. unlawful conduct within the meaning of Legislative Decree No. 231 of 8 June 2001, or violations of the Organisation and Management Model provided for by the same Decree and adopted by the Company that do not fall under the following numbers 2), 3), 4) and 5); 2. offences falling within the scope of the European Union or national acts indicated in the relevant annex to Legislative Decree No. 24/2023 or national acts constituting implementation of the European Union acts indicated in the annex to the directive (EU) 2019/1937, although not indicated in the relevant annex to Legislative Decree No. 24/2023 or, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and protection of personal data and security of networks and information systems; 3. acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary law of the European Union; 4. acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including infringements of EU competition and State aid rules, as well as infringements relating to the internal market related to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law; 5. acts or conduct that frustrate the object or purpose of the provisions of Union acts in the areas indicated in (2), (3) and (4).

WHISTLEBLOWING PROCEDURE

The Company has confirmed its entrepreneurial policy to respect the principles of legality and correctness set forth in the Code of Ethics, thereby demonstrating its extraneousness to unfair or illegal policies or conduct. This policy is set out in the Organization, Management and Control Model for the prevention of the risk of offences adopted pursuant to and for the effects indicated in Articles 6 and 7 of Legislative Decree 231/2001.

All Addressees of the Model are obliged to Report Violations of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or the private entity, within the scope of the Violations referred to in this procedure, of which they have become aware in the work context.

Such Reports must be as circumstantial as possible, made in good faith, on the basis of reasonable belief founded on precise and concordant facts.

This procedure constitutes the implementation, within the Company, of the regulatory provisions on the protection of persons who report breaches as set out in Legislative Decree no. 24/2023. This rule constitutes the primary reference for every activity contemplated hereunder.

THE REPORTS COVERED BY THIS PROCEDURE

This procedure concerns Reports of the following Violations identified in Article 2 of Legislative Decree No. 24 of 10 March 2023, namely:

1. unlawful conduct within the meaning of Legislative Decree No. 231 of 8 June 2001, or violations of the Organisation and Management Model provided for by the same Decree and adopted by the Company that do not fall under the following numbers 2), 3) 4) and 5);
2. offences falling within the scope of the European Union or national acts indicated in the relevant annex to Legislative Decree No. 24/2023 or national acts constituting implementation of the European Union acts indicated in the annex to Directive (EU) 2019/1937, although not indicated in the relevant annex to Legislative Decree No. 24/2023 or, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and protection of personal data and security of networks and information systems;
3. acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union specified in the relevant secondary law of the European Union;
4. acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including infringements of EU competition and State aid rules, as well as infringements relating to the internal market related to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
5. acts or conduct that frustrate the object or purpose of the provisions of Union acts in the areas indicated in (2), (3) and (4).

Alerts may relate to

- information, including well-founded suspicions, concerning violations committed;
- information, including well-founded suspicions, concerning violations that, on the basis of concrete evidence, might be committed;
- evidence of conduct aimed at concealing such violations.

With specific reference to the conduct referred to in paragraph 1), the following cases are mentioned by way of example:

- unlawful conduct, relevant under Legislative Decree 231/01;
- violations of the Model, of the Code of Ethics or of preventive Protocols from which a sanctioning risk for the Company may arise pursuant to the Decree;
- suspicions of violations of the Model, the Code of Ethics or the Preventive Protocols from which a sanction risk for the Company may arise under the Decree;
- corporate or business transactions for which it is suspected that a sanction risk may arise for the Company under the Decree.

This procedure also indicates the channels for making reports concerning the risks of corruptive phenomena, as referred to in the management system for the prevention of corruption (ISO 37001:2016), reports concerning issues covered by SA8000 certification (working conditions, sustainable development, social issues, etc.) and reports concerning issues covered by PdR125 certification (e.g. accidents, reports of violence or abuse, performance indicators [Key performance indicators] not in line, etc.).

Reports of breaches as referred to in number 1) can only be made through the internal reporting channel.

SCOPE OF APPLICATION

COMPANY PERIMETER

This document applies to the Addressees as identified above in chapter "Definitions".

The Whistleblowing management process set out in this document does not refer to communications of a commercial nature or to information of a purely deleterious nature that does not relate to Breaches of Legislative Decree 24/23
This procedure also does not apply to objections, claims or demands linked to a personal interest of the reporting person or of the person who has filed a complaint with the judicial or accounting authorities that relate exclusively to his or her individual employment relationships or inherent to his or her employment relationships with hierarchically superior figures.
As a general rule, the Company urges its employees to resolve any labour disputes, where possible, through dialogue, even informally, with their colleagues and/or direct supervisor.

REPORTING MANAGEMENT PROCESS

Reporting Channels [3]

Internal reporting via email

Pursuant to the law, the Company has set up its own internal reporting channel pursuant to Legislative Decree 24/2023, which guarantees the confidentiality of the identity of the Reporting Person, the Person involved and the person in any case mentioned in the Report, as well as the content of the Report and the relevant documentation.

The Company has therefore set up a computerised channel for the receipt of Reports of Violations of Legislative Decree 24/23 (rde@serviziosegnalazioni.it) managed by an external company ('external

3 In addition to the reporting or disclosure channels indicated in this procedure, Legislative Decree 24/23 also provides for the possibility for the person concerned to make a complaint to the judicial or accounting authorities

company'), appointed as Data Processor pursuant to Article 28 of the GDPR, which is responsible for receiving them and transferring them in anonymised form to the function in charge of managing the investigation.
Since the Company has adopted the Management System for the Prevention of Corruption (ISO37001:2016), the Social Accountability Certification SA8000, and the UNI/PdR 125:2022 Gender Equality Certification, it is also possible to carry out the following actions through the e-mail box, rde@serviziosegnalazioni.it :

1. reports concerning the risks of corruptive phenomena, as referred to in the management system for the prevention of corruption (ISO 37001:2016);
2. Reports on issues covered by SA8000 certification (working conditions, sustainable development, social issues, etc.);
3. reports related to PdR125 issues (e.g. incidents, reports of violence or abuse, performance indicators [Key performance indicators] not in line, etc.).

Based on the content of the report received, the external company sends the report to the competent function. In particular:

- To the Supervisory Board for Reporting Violations pursuant to Legislative Decree 24/23
- to the Anti-Bribery and Anti-Corruption Function for reporting on issues related to ISO 37001:2016 certification
- to members of the SA8000 Steering Committee for reporting on SA8000 certification;
- to the members of the UNI-PDR125/2022 Steering Committee for reports on PdR125 certification.

The external company undertakes to issue an acknowledgement of receipt within 7 days of receipt of the report and to diligently follow up on the reports received by maintaining contact with the reporting person until the report is closed.
The external company ensures adequate security measures to protect the personal data included in the Reports, guaranteeing the confidentiality of the reporting person and of all persons involved. The information on the Reports transmitted by the external company therefore does not include the personal data of the reporting person or information allowing the identity of that person to be traced.
Where a report not falling under the above-mentioned topics (e.g. complaints, claims, notifications of acts) is received at the channel rde@serviziosegnalazioni.it , the reporting channel manager informs the reporting person that he/she cannot handle the report and, in agreement with the Company, will indicate to the reporting person the appropriate channel for making the report.

INTERNAL SIGNALLING THROUGH OTHER CHANNELS

Violations pursuant to Legislative Decree 24/23
In addition to the computerised reporting channel, the Reporting Person may also make Reports of Violations pursuant to Legislative Decree 24/23:
in writing, by ordinary mail, to the address of the Company - RIZZANI DE ECCHER SPA- Via Buttrio 36 - Pozzuolo del Friuli (UD) - 33050 - Italy, by inserting the documentation relating to the report inside a sealed envelope, which - together with another envelope containing the identification data of the reporting party - must be placed inside a third sealed envelope marked "confidential to the Supervisory Board";
orally by means of a request, through the external company or directly to the Supervisory Board, for a direct meeting with the Supervisory Board set within a reasonable time. In such cases, subject to the consent of the Reporting Person (requested directly by the Supervisory Board), the internal Reporting may be documented by the authorised personnel by means of a recording on a device suitable for storage and listening, or by minutes. In the case of minutes, the Reporting Person may verify, rectify and confirm the minutes of the meeting by signing them.

Charged with the management of this channel, as well as with the management of the investigation following a report of a breach of Legislative Decree 24/23 is the Supervisory Board.
If, for the purposes of the preliminary investigation, the Supervisory Board needs to know the identity of the Whistleblower, it makes a request to the external company, which will ask the Whistleblower to consent to the sharing of his personal data with the Supervisory Board and any third parties, whose intervention is necessary for the purposes of the preliminary investigation. The free, specific, unequivocal and informed consent of the Reporting Person must be collected in writing and kept by the Surveillance Body in the documentation relating to the Report.
The members of the Supervisory Board have been duly authorised by the Company to process the personal data4 contained in internal Reports.
If the Report concerns one of the members of the Supervisory Board, please refer to Chapter 'Special Cases'.

Reporting ISO37001:2016

In addition to the computerised reporting channel, the reporting person may make reports concerning the risks of corrupt phenomena to the Anti-Bribery Department through the following channels:

- in writing, by ordinary mail, by confidential letter headed: Anti-Corruption Function of Rizzani De Eccher S.p.A.- Via Buttrio 36 - Pozzuolo del Friuli (UD) - 33050 - Italy.

The Anti-Corruption Department is in charge of managing this channel as well as .

SA8000 Reporting

In addition to the computerised reporting channel, the Reporting Person can make reports on SA8000 certification issues (e.g. working conditions, sustainable development, social issues, etc.) to the SA8000 Steering Committee through the following channels:

- in written form, through the "Complaints" box located near the Secretariat office at the company's headquarters, where only the members of the SPT-Committee have the keys to open it.
- in written form, through the specific Social Responsibility Reports section published on the company intranet Connect.
- in written form, to the following control bodies: - Certifying body SI Cert S.A.G.L, Strada Statale 18, 119/121 84047 Capaccio Paestum (SA) - IT tel. +39 0828 189.78.57 mail reclamisa8000@sicert.net; SAAS (Social Accountability Accreditation Services), 9 East 37th Street, 10th floor New York, NY 10016 - USA tel. +1-(212) -391-2106 mail saas@saasaccreditation.org.

The SA8000 Steering Committee is in charge of managing this channel as well as the investigation.

UNI-PDR125/2022 reports

In addition to the computerised reporting channel, the Reporting Person may make reports to the Steering Committee UNI-PDR125/2022 concerning PdR125 certification issues (e.g. incidents, reports of violence or abuse, performance indicators [Key performance indicators] not in line, etc.) through the following channels:

- in written form, through the "Complaints" box located near the Secretariat office at the company's headquarters, where only the members of the SPT-Committee have the keys to open it.
- The UNI-PDR125/2022 Steering Committee is responsible for the management of this channel as well as the management of the preliminary investigation.
- The Anti-Bribery Function, the SA8000 Steering Committee, the Steering Committee UNI-PDR125/2022 upon receipt of the report shall inform the Supervisory Body of the content of the

[4] The authorisation is understood to be provided pursuant to Art. 29 of Regulation (EU) 2016/679 and Art. 2-quaterdecies of Legislative Decree 196/03.

report, taking care not to disclose the personal data of the reporting person or information that allows to trace the identity of the reporting person, which may be disclosed only if necessary, in compliance with Article 12 of Legislative Decree 24/23. Where the report concerns one of the breaches relevant under Legislative Decree 24/23 it is handled by the Supervisory Body in accordance with the provisions of this procedure.

The protections and safeguards provided for in this procedure apply only in respect of reports of breaches under Legislative Decree 24/2023.

External signalling

The Reporting Person may also submit an External Report[5] to the National Anti-Corruption Authority (ANAC) if the following conditions are met:

the internal report submitted in accordance with the terms of this procedure was not followed up;

the Whistleblower has justified and substantiated reasons to believe that, if he or she made an internal report, it would not be effectively followed up, or that it could lead to the risk of retaliation;

the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

The external reporting channel set up by ANAC guarantees, in the same way as the above-mentioned internal channel defined by the Company, the confidentiality of the identity of the Reporting Person and, of the content of the report, of the Person involved and of any persons involved in the Report.

External Reports are made in written form through the computer platform made available by ANAC on its website in the section dedicated to "Whistleblowing". Whistleblowing may also be made orally through telephone lines or voice messaging systems, or, at the request of the Whistleblower, through a direct meeting set within a reasonable period of time; the methods of access to such channels are specified by ANAC on its website.

Public Disclosure

The Reporting Person is also granted the possibility of making a public disclosure[6] if one of the following conditions is met:

the Reporting Person has previously made an internal and/or external Report and no feedback has been received within the time limits laid down in this procedure[7] on the measures envisaged or taken to follow up the Report;

the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;

the Reporting Person has well-founded reasons to believe that the external Report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the Reporting Person may be in collusion with the author of the Breach or involved in the Breach.

[5] Reports of breaches relevant under Legislative Decree No. 231 of 8 June 2001, or of the Organisational, Management and Control Model adopted by the Company, provided for by the same Decree, are excluded from the application of this chapter, and may only be made through internal reporting (Article 3(2)(b) of Legislative Decree 24/23).

[6] Reports of breaches relevant under Legislative Decree No. 231 of 8 June 2001, or of the Organisational, Management and Control Model adopted by the Company, provided for by the same Decree, are excluded from the application of this chapter, and may only be made through internal reporting (Article 3(2)(b) of Legislative Decree 24/23).

[7] In compliance with the provisions of Articles 5 and 8 of Legislative Decree 24/2023 *on the "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws*".

HANDLING OF REPORTS OF VIOLATIONS PURSUANT TO LEGISLATIVE DECREE 24/23

INTERNAL REPORTING

Those who wish to make an internal written Report may do so by attaching the appropriate form in Appendix.
The Form provides the Reporting Person with a guided pathway, structured through a series of questions and requests for supporting elements, aimed at describing in a clear, precise and circumstantiated manner the situation that is the subject of the Report.
Reports must be based on precise and concordant elements of fact. The Reporting Person is requested to attach all the documentation proving the reported facts, refraining from undertaking autonomous initiatives of analysis and investigation.

RECEPTION AND ANALYSIS OF INTERNAL REPORTING

The internal reporting manager is the Supervisory Board, which handles internal Reports received ,through the channels referred to in chapter “reporting management process”, in a confidential manner, adopting verification methods suitable to protect the identity of the Reporting Person as well as that of the Persons involved.

Preliminary verification
All internal Reports received are subject to a check in order to understand whether the communication received is accompanied by the necessary information to verify its validity beforehand and to be able to initiate subsequent follow-up activities.

The Supervisory Board, also through the external company, undertakes to issue the reporting person with an acknowledgement of receipt within 7 days of receipt of the internal report.
The SB diligently follows up the Reports received, maintaining contacts with the Reporting Person, from whom it requests information if necessary. Even in this case, the Supervisory Board may make use of the external company in the event that communications are made via computer channel.

Without prejudice to the confidentiality of the information received, in the preliminary verification activities, the Supervisory Board may avail itself of the support of other structures of the Company or of specialised consultants, on the basis of the specific skills required in relation to the content of the Report under verification.
At the end of the preliminary verification, the Supervisory Board may file internal Reports:

- unsubstantiated;
- those which, on the basis of the description of the facts and the information provided by the Reporting Person, do not allow a sufficiently detailed picture to be obtained for further investigations to be undertaken to ascertain whether they are well-founded;
- those that are manifestly unfounded.

In the preliminary investigation and verification phase, the Supervisory Board:

- ensures the impartiality, fairness and accuracy of the analysis and evaluation of internal reporting;
- ensures the confidentiality of the information collected and the confidentiality of the name of the reporting person, where provided;
- undertakes not to use internal Reports beyond what is necessary to adequately follow them up. The Supervisory Board may not disclose the identity of the Reporting Person and any other information

from which such identity may be inferred, directly or indirectly, without the express consent of the Reporting Person, to persons other than those competent to receive or follow up the Reports, expressly authorised to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article *2-quaterdecies* of the Personal Data Protection Code under Legislative Decree 196/03.

Alerts that do not pass preliminary verification

Internal Reports that do not pass the preliminary stage are filed by the external company in the e-mail box where they were received and, if necessary, by the Supervisory Board in a special logical space that guarantees, by means of encryption tools, the confidentiality of the identity of the reporter, accessible only to the members of the Supervisory Board itself.

In the case of reports received in paper form, they will be stored in such a way as to guarantee the confidentiality of the personal data included therein, using appropriate security measures.

Internal Reports that do not pass the preliminary stage are accounted for in the periodic reporting described below.

In any case, the SB records the internal Reporting and the activities carried out following its receipt in the Reports and Investigations Book, always guaranteeing the confidentiality of the identity of the Reporting Person and of the Persons involved. The Reports and Investigations Book must be kept by the SB itself and made accessible only to persons authorised by the Company.

Alerts that pass preliminary verification

If the preliminary check carried out by the Supervisory Board establishes that the internal report, adequately substantiated and accompanied by evidence from which it has been possible to deduce that it is well-founded, integrates conduct that is liable to prosecution even if only disciplinary, the Supervisory Board shall

1. give immediate and reasoned information to the functions/organs in charge of applying the sanctions and disciplinary system, as set out in chapter "Sanctions system and disciplinary", so that they can self-determine on the disciplinary action to be taken also in compliance with the principles of specificity[8] , immediacy[9] and immutability[10] of the dispute if the Persons involved are Company employees[11] . Within the scope of their self-determination, such functions/bodies may carry out further investigations and checks, requesting the support of the SB, which remains the reporting Person's sole interlocutor and guarantees his/her anonymity, also possibly through the external company. Where, following further investigations and checks, such functions/bodies:
   - consider that the conduct is not objectionable, they shall immediately inform the Supervisory Board so that the latter may file the Report in the manner described above (see section on *Reports that do not pass preliminary verification*) and inform the Reporting Person of the status of the procedure;
   - decide to proceed with the objection, together with the objection, the Person concerned must be provided with appropriate privacy information pursuant to Article 14 of the GDPR and in any case within one month of the start of the processing.

[8] See Cass., 14 May 2014, No. 10662.
[9] See Cass., 15 June 2015, No 12337, Cass., S.U., 27 December 2017, No 30985, Cass. No 19256 of 17 July 2019, Cass. No 24605 of 4 November 2020,
[10] See Cass., 9 June 2016, No 11868.
[11] In such circumstances, disciplinary measures are applied in compliance with the provisions of Article 7 '*Disciplinary Sanctions*' of Law 300 of 1970 (Workers' Statute)

2. inform the management body (Board of Directors) for the assessments of their respective competences, highlighting the subject of the report, the outcome of the investigation, the possible activation of the sanctions system, as well as any corrective actions aimed at avoiding similar situations in the future.

The Supervisory Board undertakes to process internal Reports received within a reasonable time and to provide feedback on them, also through the external company, to the Reporting Person within:

- three months from the date of the acknowledgement of receipt, or failing that,
- within three months of the expiry of the seven-day period from the submission of the Report.

PENALTY SYSTEM AND DISCIPLINARY

Activation of the Sanctions and Disciplinary System

In cases where the investigations carried out reveal that the Violations covered by the Internal Reporting are well-founded, the body/function in charge of activating the Sanctions System decides what type of sanction to impose on the individuals who committed the violation.
Depending on the qualification of the Person involved and the possible labour law framework, the Disciplinary System is activated by:

- HR/AD function if he/she is an employee or manager of the company;
- Board of Directors activating the Shareholders' Meeting for consequent action, if the reported person is an auditor;
- Board of Statutory Auditors that activates the Shareholders' Meeting for consequent action, if the reported person is a Director;
- Board of Directors, if he is a member of the Supervisory Board;
- Managing Director if it is a third party.

The sanction may be graduated according to the seriousness of the offence, in compliance with the regulations applicable from time to time (e.g. labour law in the case of employees of the Company).

In the event that the Reporting Person is jointly responsible for the Breaches, preferential treatment shall be given to the latter with respect to the other jointly responsible persons, consistent with the Breach committed and the applicable discipline.

The identity of the reporting person and any other information from which this identity may be inferred, directly or indirectly, cannot be disclosed without his/her express consent. The free, specific, unequivocal and informed consent of the Reporting Person shall be collected in writing and kept by the Supervisory Board in the documentation relating to the Report.

In the context of disciplinary proceedings, the identity of the reporting person, in the absence of consent, may in any case not be disclosed where the accusation of the disciplinary charge is based on investigations that are separate from and additional to the Report, even if consequent to it.
If, on the other hand, the charge is based in whole or in part on the Report, and knowledge of the identity of the Reporting Person is indispensable for the defence of the Person concerned, the SB, where it has not already obtained the consent of the Reporting Person, shall inform the latter, by means of a written communication, of the reasons underlying the need to disclose his/her identity or other information from which it may potentially be inferred, in order to be able to fully follow up the handling of the Report, or for the purposes of the disciplinary proceedings.

If the reporting person refuses to consent to the disclosure of his or her identity, the Supervisory Board shall file the internal report without further action.

This procedure is without prejudice to the reporting person's criminal and disciplinary liability in the event of a libellous or defamatory report under the Criminal Code and Article 2043 of the Civil Code.
The behaviour of anyone who makes malicious or grossly negligent reports that turn out to be unfounded is also penalised.
Any form of abuse of this procedure, such as internal Reports that are manifestly opportunistic and/or made for the sole purpose of harming the whistleblower or other persons, and any other hypothesis of improper use or intentional instrumentalization of the Company that is the subject of this procedure, shall give rise to liability in disciplinary and other competent fora.

Therefore, when the criminal liability of the Whistleblower for the offences of defamation or slander, or civil liability in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance, the protections provided for in this procedure are not guaranteed and a disciplinary sanction[12] shall be imposed on the Whistleblower.

PROTECTING THE REPORTING PERSON AND ENFORCING PROTECTION MEASURES

Any form of Retaliation against the Reporting Person is prohibited.
Pursuant to the law, the prohibition of retaliation and, in any case, the protective measures provided for by law against the reporting person also apply:

1. to Facilitators;
2. persons in the same employment context as the reporting person, the person who has filed a complaint with the judicial or accounting authorities or the person who has made a public disclosure and who are linked to them by a stable emotional or kinship link up to the fourth degree;
3. co-workers of the reporting person or of the person who has filed a complaint with the judicial or accounting authorities or made a public disclosure, who work in the same work context as the reporting person and who have a regular and current relationship with that person;
4. entities owned by the reporting person or the person who filed a complaint with the judicial or accounting authorities or made a public disclosure, or for which those persons work, as well as entities operating in the same employment context as those persons.

The protection measures apply when at the time of the Report (internal and/or external), or the report to the judicial or accounting authorities or public disclosure, the Reporting Person:

- had reasonable grounds to believe that the information on the Breaches was true and related to violations of national or EU regulatory provisions affecting the integrity of the private entity, of which they had become aware in the work context;
- carried out the Reporting (internal and/or external) or Public Disclosure in accordance with the regulations applicable to them pursuant to Legislative Decree 24/2023.

The reasons that led the person to report or publicly disclose are irrelevant for the purposes of his or her protection.
The conditions for protection also apply in cases of (internal and/or external) Whistleblowing or reporting to the judicial or accounting authorities or anonymous public disclosures, if the Reporting Person was subsequently identified and suffered retaliation, as well as in cases of reports submitted to the competent

[12] For further details in this respect, please refer to Article 16 '*Conditions for the protection of the reporting person*'.

institutions, bodies and organs of the European Union, in accordance with the conditions set out in this Procedure (as well as in Article 6 of Legislative Decree 24/2023)

The adoption of discriminatory measures against Whistleblowers may be communicated to the ANAC, which in turn will inform the National Labour Inspectorate for measures within its competence.

Acts taken in violation of the prohibition of Retaliation are null and void, and the Whistleblower who has been dismissed as a result of the Whistleblowing (internal and/or external), Public Disclosure or Whistleblowing is entitled to be reinstated in his/her job.
In the context of judicial or administrative proceedings or extrajudicial disputes concerning the ascertainment of the prohibited conduct, acts or omissions against the Whistleblower, it is presumed that such conduct or acts were committed as a result of the Whistleblowing (internal and/or external), public disclosure or complaint. Pursuant to the law, the burden of proving that such conduct or acts are motivated by reasons unrelated to the Reporting (internal and/or external), the Public Disclosure or the Whistleblowing is on the person who has carried them out.
Moreover, in the event of a claim for damages submitted to the judicial authority by the Whistleblower, if he/she proves that he/she has made a Report (internal and/or external), a Public Disclosure or a Complaint to the judicial or accounting authority and has suffered damage, it is presumed, unless proven otherwise, that the damage is a consequence thereof.

LIMITATIONS OF LIABILITY

Pursuant to the law, a reporting person who discloses or disseminates information on Breaches covered by an obligation of secrecy, other than that set out in Article 1(3) of Legislative Decree no. 24/2023[13] , or relating to the protection of copyright or the protection of personal data, or who discloses or disseminates information on Breaches offending the reputation of the person involved or reported when, at the time of disclosure or dissemination, there were reasonable grounds for believing that the disclosure or dissemination of the same information was necessary to disclose the Breach and the Reporting (internal and/or external), Public Disclosure or the report to the judicial or accounting authorities was made in compliance with the provisions of Legislative Decree 24/2023.

In such cases, any further liability, including civil or administrative liability, is also excluded.

Unless the act constitutes a criminal offence, the Company or the Reporting Person shall not incur any liability, including civil or administrative liability, for the acquisition of or access to the Breach Information.

In any event, criminal liability and any other liability, including civil or administrative liability, is not excluded for conduct, acts or omissions that are not related to the Reporting (internal and/or external), to the denunciation to the judicial or accounting authorities or to the Public Disclosure or that are not strictly necessary to disclose the Breach.

[13] Article 1(3) of Legislative Decree 24/2023 provides: "This is *without prejudice to the application of national or European Union provisions on:*
(a) classified information;
(b) forensic and medical professional secrecy;
(c) secrecy of court deliberations

STORAGE AND ARCHIVING

The reports received are kept for as long as necessary for the processing of the report, in compliance with the confidentiality obligations provided for by the type of report received and with the principle laid down in Article 5(1)(e) of Regulation (EU) 2016/679.
With reference to the disciplinary sanctioning process, resulting from the report, the competent corporate functions file the documentation relating to the sanctioning and disciplinary process. The Supervisory Board must be informed of any sanctions.

REPORTING

The Supervisory Board reports annually on the proper functioning of the internal reporting systems, indicating in its report the aggregate information on the results of the activity carried out and on the follow-up given to the internal Reports received.
In drawing up this report, the Supervisory Board is required to comply with the provisions of the rules on the protection of the identity of the reporting person and of the applicable legislation on the protection of personal data.

SPECIAL CASES

Where the internal report concerns a member of the Supervisory Board, it shall be handled in accordance with the provisions of this procedure, but the reported member shall abstain from participating in the work and decisions of the Supervisory Board.
If the internal report containing serious, precise and concordant elements concerns more than one member of the Supervisory Board, the Manager of the reporting channel shall forward it to the Board of Directors, by handing over any supporting documentation to the Chairman of the Board of Directors.

The Board of Directors, having consulted with the Board of Statutory Auditors, after collectively assessing whether the Internal Report is accompanied by the necessary information to preliminarily verify its validity and to be able to initiate the subsequent in-depth investigations, follows it up by carrying out the preliminary investigation, also by availing itself of the company's expertise and, where appropriate, of specialised consultants, always in compliance with the confidentiality of the relevant regulations and the provisions contained in this document.
The preliminary investigation follows the procedure described in this procedure.
The decision of the Board of Directors is formalised by means of a written resolution.

RESOLUTIONS OF THE SUPERVISORY BOARD

The Supervisory Board decides by a majority of those present at the meeting. The meeting of the Supervisory Board is valid if at least half of its members are present.
In the event of a tie, the vote of the Chairman of the Supervisory Board, if present, prevails.
The Supervisory Board is convened by the President or one of its members and, specifically, by the person who has been informed of the receipt of the Report.
The summons must be issued promptly, indicatively within 3 days of receipt of the Report, and in any case within a timeframe to ensure feedback to the Reporting Person within 7 days.
The meeting may also be held by video or teleconference.

AND RESPONSIBILITIES

It is the responsibility of the external company to manage the computer channel established for receiving Reports.

It is the responsibility of the Supervisory Board to manage and archive Reports of Violations related to Legislative Decree 24/23.
It is the responsibility of the Anti-Corruption Function to manage and archive reports related to issues concerning ISO 37001:2016 certification.
It is the responsibility of the members of the SA8000 Steering Committee to manage and archive reports related to SA8000 certification issues.
It is the responsibility of the members of the UNI-PDR125/2022 Steering Committee to manage and archive reports related to PdR125 certification.

DISTRIBUTION AND STORAGE

This document is available in the company's information system.

REPORT FORM

It is recommended that you enclose any documentation that you think may be useful to substantiate the Report; if the Report is made verbally, such documentation may be handed over directly.

DATA OF THE REPORTING PERSON

First name and surname *(non-compulsory data)* _____
Structure of affiliation and qualification *(non-mandatory data)* _____
Chosen contact channels (e.g. private e-mail address, telephone number, etc.)
Does the Reporting Person have a private interest related to the Report? Yes No
Specify the nature of the private interest attached to the Report

Is the reporting person co-responsible for the violations he/she reports? Yes No

REPORTED OFFENCE

Period/date when the event occurred _____
Area of business operations to which the event may relate_____
Subjects involved:

Interior	Exteriors

Description of the fact being reported

Other persons who may report on the facts to be reported

Interior	Exteriors

Other parties to whom the Report of Fact was forwarded? Yes No
Specify which subjects and when

Data Signature

INFORMATION PURSUANT TO ARTICLE 13 OF REGULATION (EU) 679/2016
on the processing of personal data in the context of alerts

Pursuant to Article 13 of Regulation (EU) 2016/679 (*General Data Protection Regulation*, hereinafter "GDPR") and the applicable data protection legislation, Rizzani De Eccher S.p.A. informs you of the processing of personal data concerning you in the context of the management of reports. Personal data will be processed compliance with the regulations and in accordance with the principles of fairness, lawfulness and transparency by personnel authorised by Rizzani De Eccher S.p.A. pursuant to Article 29 of the GDPR and Article 2-quaterdecies of the Personal Data Protection Code (Legislative Decree 196/2003).

1. Data controller
The data controller of personal data is Rizzani de Eccher S.p.A. (hereinafter also referred to as the "Company" or "Data Controller") with registered office in Via Buttrio 36, 33050, Pozzuolo del Friuli (UD), which can be contacted at the e-mail address mail@rde.it

2. Purpose of processing and legal basis
The personal data referred to you shall be processed for the purpose of handling the report received and for carrying out the necessary investigative activities aimed at verifying the justification of what has been reported, as well as, where applicable, for taking appropriate corrective measures and introducing appropriate disciplinary and/or judicial action against those responsible for the violations.
For each area, the body in charge of handling the report, a legitimising legal basis and a retention period have been identified.
For each reporting area, specific channels for reporting have been identified.
The report sent via computer channel torde@serviziosegnalazioni.it may relate to the areas summarised in the table below

Reference regulations	Reporting body	Legal basis	Storage time
Whistleblowing - Legislative Decree 24/2023	Supervisory Board	fulfilment of a legal obligation to which the Holder is subject, specifically, provided for in Legislative Decree 231/2001, Law 179/2017 and Legislative Decree 24/2023	no later than five years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in Article 12 of this Legislative Decree 24/2023 and the principle set out in Article 5(1)(e) of the GDPR and Article 3(1)(e) of Legislative Decree No. 51 of 2018
ISO 37001	Anti-Corruption Function	fulfilment of a legal obligation to which the Controller is subject or, residually, where there is no legal obligation to handle the report, a legitimate interest related to the management of the process subject to certification.	5 years from receipt for the purpose of documenting its management, except for legal defence needs.
Harassment and Discrimination Reporting - PDR 125	Guidance Committee UNI-PDR125/2022	fulfilment of a legal obligation to which the Controller is subject	5 years from receipt in order to document its management.
SA 8000	SA8000 Steering Committee	fulfilment of a legal obligation to which the Controller is subject or, residually, where there is no legal obligation to handle the report, a legitimate interest related to the management of the process subject to certification.	5 years from receipt in order to document its management, except for legal defence needs.

3. Categories of data recipients
The personal data provided are processed by the body in charge of handling the report and, for reports sent to rde@serviziosegnalazioni.itby an external person specifically authorised pursuant to Article 28 of the GDPR by the Data Controller and appointed to follow up and respond to the reports received, in accordance with the provisions of the above-mentioned reference regulations.
The data will not be subject to dissemination but may, where appropriate, be passed on to the judicial authorities.
None of the data collected will be disclosed to third countries, i.e. countries outside the European Economic Area (EEA).

4. Storage time criteria
Internal reports and related documentation will be kept for the time necessary for the processing of the report identified above. Once the maximum period of five years has elapsed, the information relating to the report may be retained by the Company in order to guarantee and preserve its right of defence and to provide evidence, where required, of the proper handling of the reports received. In this case, the personal data referring to you or in any case relating both to the person making the report and to the Persons involved,

indicated as possibly responsible for the unlawful conduct, as well as to those who are for various reasons involved in the reports will be anonymised.

5. Modalities of data processing

Your personal data will be processed exclusively by staff expressly authorised and instructed to do so, in such a way as to guarantee the confidentiality of the identity of the Reporting Person and of the content of internal reports and related documentation, adopting appropriate technical and organisational measures to protect them against unauthorised or unlawful access, destruction, loss of integrity and confidentiality, even accidental.

6. Rights of data subjects

The rights referred to in Articles 15-22 of the GDPR may be exercised, within the limits of the provisions of Article *2-undecies*, para. 3, of Legislative Decree No. 196/2003, by contacting the Data Controller using the contacts indicated above. In particular, the rights identified above may not be exercised by means of a request to the Data Controller, or by means of a complaint pursuant to Article 77 of the GDPR to the Guarantor Authority, where the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the person reporting breaches of which he/she has become aware by reason of his/her employment relationship or functions performed. The exercise of the aforesaid rights may, in any case, be delayed, limited or excluded by reasoned notice given without delay by the Data Controller, unless such notice might jeopardise the purpose of the limitation, for the time and within the limits in which this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the Reporting Person, the Person Involved or the persons involved in the reports. In such cases, pursuant to Article 2-undecies(3) of Legislative Decree No. 196/2003, you are entitled to exercise the aforementioned rights through the Garante Authority in the manner set out in Article 160 of the aforementioned legislative decree. In cases where you believe that the processing of your personal data is in breach of the GDPR, you may lodge a complaint with the Guarantor Authority, as provided for in Article 77 of the GDPR itself (with the exclusion of the limitations to the exercise of the rights set out above and provided for in Article *2-undecies*, para. 3, of Legislative Decree no. 196/2003), or you may take legal action (Article 79 of the GDPR).