STI
ENGINEERING
Design&Consulting

OBJECT

ORGANISATION, MANAGEMENT AND CONTROL MODEL

in accordance with the Legislative Decree 231/01 (*)

DOCUMENT TITLE

GENERAL PART

MOG PG ED. 00

STI Engineering S.r.l.
Via Rodeano, 48
33038 S. Daniele del Friuli (Ud) - Italy
VAT ID 02118550306
t. +39 0432 941303

info.
www.sti-corporate.com/sti-engineering
Company subject to the Management and Coordination Activities of STI Corporate S.p.A.

TABLE OF DOCUMENT REVISIONS/UPDATES		
Rev.	**Document Date**	**Description of modifications and updates**
00	10/10/2019	First issue
01	20/04/2023	Update
02	20/04/2024	Update

(*) This document has been developed in accordance with Legislative Decree No. 231 dd. June 8, 2001 "Discipline of Administrative Liability of Legal Persons, Organizations and Associations, including those without legal personality, pursuant to Article 11 of Law No. 300 dd. September 29, 2000".

TABLE OF CONTENTS

1. Foreword 4
2. Glossary 4
3. Regulatory Framework and Purpose of the Organization, Management and Control Model (MOG) 5
   3.1. Regulatory Framework and General Purposes 5
   3.2. Adoption of the Model by the Company 8
4. Basic Principles 9
   4.1. Segregation of Duties 9
   4.2. Control and Traceability of Operations 10
   4.3. Information and Training 10
5. Recipients of the MOG (Organization, Management and Control Model) 11
6. Structure of the MOG and Responsibilities 12
   6.1. Types and Coding of Documents 12
   6.2. Structure of the MOG 13
   6.3. Responsibilities for the Approval, Adoption, Implementation, and Modification of the MOG 14
   6.4. Construction and Update of the MOG 14
7. Violation Reporting System (Whistleblowing) 18
   7.1. Scope of Application 19
   7.2. Responsibilities of the Receiver 19
   7.3. Content of the Report and Reporting Methods 20
   7.4. Handling the Report 20
   7.5. Whistleblower Protection Measures 21
8. Sanction System 23
   8.1. Scope of Application 24
   8.2. Responsibility for Application 25
   8.3. Operational Modalities for applying the Sanction System 25

Annexes

A_MOG PG_01 Company Presentation
A_MOG PG_02 List of examples of contractual clauses
A_MOG PG_03 Occupational Health and Safety Policy
A_MOG PG_04 Regulations for the use of the IT system
M_MOG PG_01 List of Organization, Management and Control Model Documents
M_MOG PG_02 Reporting Form

1. Foreword

Legislative Decree 8 June 2001, n. 231 (hereinafter also "Legislative Decree 231"), introduced into the Italian legal system the liability of Entities for offences resulting from the commission of a crime.

This is an autonomous liability system, characterized by prerequisites and consequences that are distinct from those provided for the criminal liability of the natural person.

The Decree provides for the possibility that the Entity may be exempted from such responsibilities, if it voluntarily adopts a suitable Organization, Management and Control Model (hereinafter MOG) consistent with the principles and methods defined by the Decree itself.

The Decree also provides that the MOG may be adopted by the Entity taking as a basis the codes of conduct drawn up by the associations representing the entities, communicated to the Ministry of Justice.

The purpose of this document is to illustrate the MOG voluntarily adopted by the Company, describing in detail, after a brief presentation of the regulatory framework of reference:

- the reasons that inspired its adoption;
- the purposes and basic principles;
- the documents that constitute the structure of the MOG;
- the methods followed for its definition, the approval responsibilities and the updating methods;
- the methods defined by the Company for reporting violations to the MOG (whistleblowing);
- the sanction system defined by the Company in the event of violation of the principles and rules expressed by the MOG and its Protocols.

2. Glossary

Below are some terms that are frequently used in the various documents that make up the Organization, Management and Control Model adopted by the Company:

Term	Definition
Risk Area	the process, operation, act, or set of operations and acts, which may expose the Company to the risk of committing a crime
Sensitive Activities	individual activities of the Company, primary or instrumental, which present (abstract) risks of committing one of the crimes that presuppose the administrative liability of the entity pursuant to Legislative Decree 231/01
External Collaborators	all external collaborators considered as a whole, such as consultants, partners, suppliers
Recipients	all the subjects to whom the Organization, Management and Control Model is addressed, i.e. employees, collaborators, administrative bodies, agents,

Term	Definition
	attorneys, outsourcers, other subjects with whom the Company comes into contact in the performance of business relations
Supervisory Body (or OdV)	the Body provided for by art. 6 of the Legislative Decree, which has the task of supervising the functioning and compliance with the Organization, 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" and freelancers who have received an assignment from the Company
Top Management	the persons referred to in Article 5, paragraph 1, letter a) of Legislative Decree 231, or the persons who hold representative, administrative or management roles in the Company or in one of its organizational units with financial and functional autonomy; in particular, the members of the Board of Directors, the President, any managers and attorneys
Personnel subject to the direction of others	the persons referred to in Article 5, paragraph 1, letter b) of Legislative Decree 231, or all Personnel who operate under the direction or supervision of Top Management Personnel
Protocol	the organizational, physical and/or logical measure provided for by the Model in order to prevent the commission of the Crimes with binding effect issued within the Company (for example: procedures, organizational provisions, circulars, service orders, notices to personnel, etc.)
Crime or Predicate Crime	the set of crimes, or the single crime, referred to in Legislative Decree 231/2001 and subsequent amendments.
Report	any information concerning alleged findings, irregularities, violations, reprehensible behaviours and facts with respect to the contents of the Code of Ethics and the Organizational Model

3. Regulatory Framework and Purpose of the Organization, Management and Control Model (MOG)

3.1. Regulatory Framework and General Purposes

Legislative Decree No. 231 of June 8, 2001, establishes the administrative liability of entities in criminal proceedings, including legal entities, companies, or associations, resulting from the commission of criminal offenses, aligning with a process initiated by the European Union regarding the definition of corporate responsibilities.

The decree, which came into effect on July 4, 2001, introduces for the first time in Italy a specific form of liability for entities concerning certain crimes committed in the interest or for the benefit of the entities by their personnel (top management, employees, etc.). This liability, which does not exist if the offenders act solely in their own interest or that of third parties, does not replace the liability of the natural person who committed the unlawful act but is added to it.

According to Article 5 of Legislative Decree 231, those potentially exposed to committing criminally relevant acts include:

- **Top management personnel**, i.e., individuals holding representation, administrative, or managerial roles within the entity or a unit with financial and functional autonomy, as well as those who exercise management and control functions, even de facto;
- **Subordinate personnel**, i.e., individuals under the direction or supervision of one of the subjects indicated above.

This liability regime involves the punishment of certain criminal offenses, affecting the assets of entities that have benefited from the commission of such offenses. In the event of an offense, a monetary penalty is always imposed, and in more severe cases, additional severe prohibitive measures may be applied, such as the suspension or revocation of licenses and concessions, the prohibition of business operations, the ban on contracts with the Public Administration, exclusion or revocation of funding and contributions, prohibition of advertising goods and services, up to the appointment of a judicial commissioner for the company.

Entities may be held liable only in relation to specific crimes, known as predicate offenses (hereinafter simply referred to as offenses), identified by the Decree and subsequent laws explicitly referencing the Decree's provisions. Over time, the list of offenses has been expanded and modified by subsequent legislative measures.

Entities may also be held liable in Italy for relevant offenses under Legislative Decree 231 committed abroad (Article 4 of the Decree).

However, Article 6 of Legislative Decree 231 states that an entity is not liable for the offense (i.e., a specific form of exemption from liability is provided) if it can demonstrate that:

a) The governing body has adopted and effectively implemented, prior to the commission of the act, organizational and management models (MOGs) capable of preventing crimes of the type that occurred.

b) The task of overseeing the functioning and compliance with the models and ensuring their updating has been entrusted to a body within the entity with autonomous powers of initiative and control (the so-called Supervisory Body or ODV), which in smaller entities may coincide with the governing body itself.

c) The individuals committed the crime by fraudulently circumventing the organizational and management models.

d) There was no failure or insufficiency in the supervision by the body mentioned in point b).

The same article also establishes that MOGs can be adopted based on codes of conduct drawn up by representative associations of entities and communicated to the Ministries of Justice. For the adoption of the MOG to exempt the entity from liability, **it must be effectively implemented**. In other words, the specific culpability of the entity is established when the offense committed by one of its members or subordinates is part of a business decision or when it is a consequence of the entity's failure to adopt an MOG capable of preventing offenses of the type that occurred or due to inadequate supervision by the bodies with control powers.

If the crime is committed by individuals subject to the direction or supervision of the top management, the entity will only be liable if there is a failure in the obligations of direction and supervision. Such failure is excluded, as specified above, if the entity has adopted, prior to the commission of the offense, an MOG capable of preventing offenses of the type that occurred.

Within this regulatory framework, MOGs, for the purpose of crime prevention, must:

- Identify activities at risk of crime.
- Provide specific procedures for crime prevention.
- Identify methods for managing financial resources to prevent crimes.
- Include obligations to inform the body responsible for monitoring the functioning and compliance with the models.
- Establish a reporting channel for violations of the model in accordance with the law.
- Introduce an internal disciplinary system capable of sanctioning non-compliance with the measures specified in the model.

With the entry into force of the Business Crisis and Insolvency Code (Legislative Decree 14/2019), which amended Article 2086, paragraph 2, of the Civil Code, requiring entrepreneurs to adopt an organizational, accounting, and administrative structure capable of detecting signs of a business crisis, the safeguards and procedures outlined in the MOGs represent an ideal tool for the self-control purposes envisaged by the regulation.

The effectiveness and efficiency of the MOGs in business management can also serve as an important defensive element for directors who may be called to account for their managerial actions before shareholders, creditors, and the judiciary.

Moreover, with the enactment of the New Procurement Code (Legislative Decree 36/2023), the legislator, while raising the thresholds for direct awarding of service and work contracts, emphasized the reliability and transparency requirements of participating companies. These companies can thus use MOGs, including an

ethical code and a sanctioning system, as evidence of their qualifications, even in cases where exclusion from the tender may occur (principle of so-called self-cleaning).

The general purposes of the MOGs are therefore:

1. To **prevent and reasonably limit** potential risks associated with business activities, particularly in reducing any illegal behaviour.
2. To **make everyone** operating in the name and on behalf of the Company **aware**, in risk-prone areas, that violations of the provisions contained in the MOG can result in criminal and administrative penalties not only for themselves but also for the Company.
3. To **reiterate that the Company does not tolerate any illegal behaviour**, regardless of the purpose, as such behaviour, in addition to violating current laws, is contrary to the ethical and social principles the Company adheres to.
4. To **equip the Company with an adequate** organizational, accounting, and administrative control **structure** to detect signs of business crises and enable the timely activation of procedures for addressing the crisis according to legal models, while preventing the commission of crimes naturally linked to pathological corporate situations (primarily corporate and tax crimes).

3.2. Adoption of the Model by the Company

The Company deemed it necessary to adopt a MOG in accordance with Legislative Decree 231/2001, which was drafted based on the Guidelines developed by Confindustria (2021 edition). This decision aligns with a broader strategic plan that considers management control and the control of operational, legal, and reputational risks as fundamental pillars of its business model, reflecting the importance the Company places on compliance with legality and ethics in business.

The general principles underlying the MOG are aligned with the Company's longstanding commitment to creating and maintaining a governance system adhering to principles of quality, customer satisfaction, high ethical standards, and efficient business management. Additionally, they ensure the Company's activities comply with current legislation and protect the interests of its stakeholders.

The Company also believes that the adoption of a MOG, together with the simultaneous issuance of the Code of Ethics as its fundamental component, serves as an effective means of raising awareness among all employees and other parties involved with the Company (Clients, Suppliers, Partners, etc., collectively referred to as Recipients).

In line with the aforementioned principles, the Company intends to implement a system of controls, organizational safeguards, and decision-making protocols designed to guide the conduct of employees and collaborators towards full compliance with applicable laws and internal regulations.

The adoption of these tools aims to ensure that all involved parties engage in their activities with correct and

transparent behaviour, consistent with the ethical and social values the Company upholds in pursuing its corporate objectives. Additionally, these measures are designed to prevent the risks of committing the offenses contemplated by the Decree.

4. Basic Principles

The MOG adopted by the Company establishes the application of several fundamental principles such as:

- Segregation of duties
- Control and traceability of operations
- Information and training for the Recipients

These principles are integrated into a system of organizational, operational, and control procedures that identify areas and processes subject to potential risks in the conduct of business activities, particularly those involving the risk of offenses under the Decree.

The MOG therefore defines an internal regulatory system aimed at planning the formation and implementation of the Company's decisions in relation to the risks/offenses to be prevented through:

1. A complex system composed of a Code of Ethics, which sets general guidelines, and formalized procedures (so-called Protocols), aimed at detailing the methods for making and implementing decisions in “sensitive” areas.
2. A system of delegations and corporate powers ensuring a clear and transparent representation of the process for decision-making and implementation within the Company.
3. A set of coherent organizational structures designed to inspire and control proper behaviour, ensuring clear and systematic task assignment, applying appropriate segregation of functions, and ensuring that the intended organizational structures are effectively implemented.

The following sections describe these principles in their practical application.

4.1. Segregation of Duties

The distribution of responsibilities is pre-emptive and balanced, based on the principle of separation of functions to avoid the mixing of potentially incompatible roles or excessive concentration of responsibilities and powers in a single individual. Specifically, separation of activities and responsibilities is ensured between those who authorize, those who execute, and those who control a particular operation in sensitive activities.

Authorization and signing powers are clearly defined and known within the Company, consistent with assigned organizational and managerial responsibilities, and specify, where required, approval thresholds for expenses. To this end, the preparation and internal distribution of an up-to-date organizational chart, which graphically represents the above, is significant.

4.2. Control and Traceability of Operations

Every sensitive operation is documented using adequate support (paper or electronic), allowing tracking of its characteristics and reasons, as well as identifying who authorized, performed, recorded, and, if applicable, verified the operation. The ability to delete or destroy recorded data is regulated. The traceability of operations ensures the possibility of a control and supervision system over sensitive operations, which must be periodically conducted by competent functions.

The implementation of a control system is proportionate to the organization and size of the company. The Company protects itself by adopting the control components to the extent of its capabilities to achieve an acceptable level of risk, ensuring that the "costs" of implemented controls do not exceed the value of the resource to be protected. Therefore, these preventive tools, even if not all adopted, should integrate into an organic system where the weakness or absence of one component is compensated by the strengthening of another, creating a form of balance.

In this regard, the presence of a communication system and the archiving of communications and information circulation, both in paper and electronic formats, is significant.

4.3. Information and Training

The Company promotes the awareness of the MOG, related internal procedures, and their updates among all Recipients, who are therefore required to know its contents, observe them, and contribute to their specific and precise implementation.

The training and information activities must ensure that the staff:

- Have received the Company's Code of Ethics;
- Have been adequately informed through comprehensive, effective, clear, detailed, and regularly repeated communication regarding:
  - Organizational powers (representation and signing powers), proxies, hierarchical lines (organizational chart), and procedures of the Special Part;
  - Information flows and all that contributes to transparency in daily operations.

To ensure widespread dissemination of the MOG and its components, especially the Code of Ethics, both internally and externally, the Company ensures their publication on the corporate website, according to the defined procedures.

For the internal dissemination of the MOG, a specific area of the company's IT network dedicated to the topic is available and periodically updated. This area contains not only the documents that make up the previously described information set but also forms and tools for reporting to the ODV and any other relevant documentation.

The Company, aware of the importance of training and information aspects (as a protocol of primary

importance), works to ensure that the staff are knowledgeable about the contents of the Decree and the obligations arising from it.

Information and training activities are established and carried out both at the time of hiring or the start of the relationship and in the event of changes in the individual's function, changes in the MOG, or other factual or legal circumstances that necessitate it to ensure the proper application of the provisions of the Decree.

Specifically, following the approval of the updated version of this document, the following actions are expected:

- An initial communication to all staff in place at the time of adoption about the adoption of this document.
- Delivery to new hires of an information set defined by the Company, containing references to the MOG and related Procedures, in accordance with company practices adopted for other regulations, such as privacy and information security.
- Signing by Employees of a specific declaration of acknowledgment and acceptance.
- Specific training activities planned for the Heads of company functions and services.

To other Recipients, particularly suppliers, consultants, and partners, specific information on the policies and procedures adopted by the Company based on the MOG, the Code of Ethics, and the consequences of conduct contrary to the provisions of the MOG or otherwise contrary to the Code of Ethics or applicable laws may have on contractual relationships is provided by the functions with institutional contacts with them, under the coordination of the ODV.

Where possible, specific clauses are included in contractual texts to regulate such consequences, such as termination clauses or rights of withdrawal in the event of conduct contrary to the norms of the Code of Ethics and/or MOG Procedures.

5. Recipients of the MOG (Organization, Management and Control Model)

The recipients of the prescriptions of the MOG are, in general, all stakeholders with whom the Company interacts in the course of business relations, such as:

- **The Directors and all Corporate Bodies** (Directors and Statutory Auditors)
- **Function Directors**
- **All Company employees**, including collaborators, consultants, proxies, and those under others' direction, whether employees or not
- **The Supervisory Body**

All Recipients must comply with the prescriptions of the MOG and the Code of Ethics, as well as the laws and regulations in force.

In particular, Top Management, or those who hold positions of representation, administration, or management within

the Company or one of its organizational units with financial and functional autonomy (members of the Board of Directors, the President, any general managers, and proxies), are responsible for:

- Ensuring the information, training, and awareness of their subordinates regarding the behaviour to be followed in the performance of their duties.
- Respecting the principle of transparency in making all corporate decisions.
- Exercising control and supervision over subordinates. This form of control is particularly relevant for those who interact with Public Entities, Authorities, and public service officers.
- Ensuring full respect for individual rights.
- Considering the possibility of terminating contracts with third parties if they become aware of behaviours and/or proceedings that are subject to the application of Legislative Decree 231/2001.

By adopting the MOG, the Company declares that it will not initiate or continue any business relationship with third parties who do not intend to adhere to the principles of the Code of Ethics, nor will it continue relationships with those who violate these principles.

Therefore, employees responsible for company functions that establish and manage business relationships with these third parties are obligated to inform them of the adoption of the MOG and the Code of Ethics, as well as to ensure that the principles contained therein are accepted and respected.

6. Structure of the MOG and Responsibilities

6.1. Types and Coding of Documents

The documents are classified into three categories:

1) **Basic Documents**: This category includes the fundamental and mandatory elements of the MOG:
   - General Part
   - Code of Ethics
   - Supervisory and Control Body – Regulation
   - Crimes and Risk Assessment
   - Special Part

   These documents define the basic structure of the MOG and are subject to infrequent modifications, mainly due to adjustments to the current legislation.

2) **Attachments to Basic Documents:** These are supplementary documents to the corresponding basic documents, specifically defined in relation to the company's reality.

3) **Forms**: These are attached to the corresponding basic documents and serve the operational purpose of providing evidence of the activities carried out once completed.

All MOG documents contain the following identifying elements:

- Document Code: Includes the initials of the reference Basic Document and, if it is an attachment, the identifying letter of the specific type (A for Attachment, M for Module).
- Date of Issue: The date the document is issued by the Administrative Body.
- Revision Number: A progressive number starting from the initial issue.

All documents comprising the company's MOG are listed in the "*MOG Document List" form, M_MOG PG_01*, which is monitored by the Administrative Body.

6.2. Structure of the MOG

The components of the MOG, in compliance with the provisions of Legislative Decree 231, are as follows:

- **General Part, MOG_PG:** This document, referencing regulatory provisions, outlines the reasons for the Company's voluntary adoption of the MOG. It describes the structure and responsibilities for its adoption and modifications, defines the methods for reporting crimes, and establishes the related sanction system. The documents attached to the General Part describe the organizational reality of the Company *(Company Presentation, A_MOG PG_01)* or address specific topics of interest to the Company covered by a specific document (e.g., the *Security Policy, A_MOG PG_02*).
- **Code of Ethics, MOG_CE:** A document that identifies the fundamental ethical values that all Recipients of the MOG must respect in the performance of their activities.
- **Supervisory and Control Body – Regulation, MOG_ODV:** This document details the operation of this body, which is explicitly required by the law, with specific duties of supervising the functioning, effectiveness, and compliance with the MOG as well as updating it.
- **Crimes and Risk Assessment, (MOG_RRA):** This section outlines the types of crimes specified in the Decree and describes the methodology used for risk assessment for each crime. The attached documents include the following elements:
  - A summary list of the crimes applicable to the Company, along with the corresponding risk level determined from the assessment and the rationale behind it.
  - A mapping of the company's processes, identifying key company figures and their respective roles (decision-making, operational, monitoring), as well as an evaluation of the existing controls.
  - The assessment of the risk level, considering factors such as significance, probability, and impact, along with illustrative examples of how crimes could be committed.
  - A comprehensive list of crimes under current law, along with the corresponding penalties.
- **Special Part and Specific Parts for Risky Business Processes, (MOG_PS):** These special sections detail, for each process identified as relevant within the Company, the potential crimes

involved in the process, the functions affected, the general principles applicable to the process, the specific procedures and protocols related to risky activities, and the types of controls overseen by the Supervisory Body (ODV).

6.3. Responsibilities for the Approval, Adoption, Implementation, and Modification of the MOG

According to Article 6, paragraph 1, letter a) of the Decree, the adoption and effective implementation of the MOG are the responsibilities of the executive management of the company.

The Administrative Body, therefore, holds the responsibility and authority to approve, integrate, and modify the core principles outlined in this document and its related annexes, which form an integral part of the MOG adopted by the Company. Thus, all decisions regarding changes and additions to the MOG fall under the jurisdiction of the Company's Administrative Body, albeit based on recommendations from the Supervisory Body (ODV) (as detailed in the document ***"Supervisory and Control Body – Regulations, MOG_ODV***").

The initiative for updates or integrations to the Code of Ethics can also come from other stakeholders, who are actively involved in the application of the principles and methods outlined therein, and whose input and reporting of any shortcomings the Company encourages. The Administrative Body is responsible for ensuring the implementation of the MOG, by evaluating and approving the necessary actions to implement its fundamental elements, with the support and recommendations of the ODV.

The Administrative Body must also ensure the implementation and actual adherence to the protocols in sensitive (or "crime-risk") business areas, in anticipation of future adjustment needs, with the involvement of functional managers concerning the sensitive activities they oversee.

Substantial modifications may include, but are not limited to: the addition of further Special Parts; the removal of certain parts of the Model; changes in the tasks or composition of the ODV; amendments to the list of information related to official acts that must be mandatorily communicated to the ODV or the Shareholders' Meeting; updates to the MOG following a reorganization of the company structure or due to legislative changes, particularly those affecting D. Lgs. 231/01.

Formal changes could include, for example, those resulting from the renaming of certain corporate functions, or the consolidation or separation of procedures outlined in the Model, provided that the substantive content remains unchanged.

6.4. Construction and Update of the MOG

The work of creating/updating the MOG consists of the following phases:

1) Collection and analysis of information, through viewing documentation and conducting interviews with the Managers of the various company processes.
2) Mapping of activities and identification of applicable crimes.

3) Risk assessment.

4) Definition of the special parts and procedures.

based on the fundamental principles of documentation and verifiability of all activities, so as to allow understanding and reconstruction of what has been achieved, as well as consistency with the dictates of Legislative Decree 231/2001 and described below with specific reference to the construction of the Company's MOG.

6.4.1. Phase 1: collection and analysis of documentation

For the creation and updates of the MOG, the following reference documents are examined (illustrative list):

- Deed of Incorporation and Company Statute.
- Updated Chamber of Commerce certificate.
- Updated Chamber of Commerce Registration.
- Powers of Attorney and Delegations Granted to Administrators and Third Parties.
- Operational Regulations and Formalized Procedures, with particular attention to documents governing internal relationships within the Company.
- Minutes of Shareholders' Meetings.
- Latest Approved Financial Statements.
- Organizational Chart and Job Descriptions.
- Workplace Safety Control System.
- Environmental Control System.
- Any Legal Proceedings Involving the Company and Individuals.

These documents constitute an information platform of the structure and operations of the Company, as well as the distribution of powers and responsibilities and are complemented by interviews and field analyses to acquire further elements of knowledge of the company reality.

6.4.2. Phase 2: Mapping of activities and identification of applicable crimes

This phase catalogues all business processes, particularly focusing on those considered sensitive under the Decree. It also involves verifying the distribution of responsibilities within the organization and analysing the presence of internal control mechanisms (formalized procedures, delegations, types of existing controls, etc.).

In this phase, based on the Company's activities, applicable crimes are identified, excluding those with a negligible probability of occurrence or where there are no concrete conditions for an interest or advantage to the Company.

6.4.3. Phase 3: Risk Assessment

This phase involves evaluating the risk of crimes for the Company as a whole in terms of:

- **Applicability of the Crimes to the Specific Process**: Each crime is classified based on the likelihood of it occurring. Although it is abstractly unlikely that a crime could not be committed within the organization, crimes are distinguished as follows for applicability assessment: Applicable = YES: Crimes that can realistically be committed in the company. Applicable = NO: Crimes with a low probability of being committed or those with no foreseeable correlation with the company's interests or benefits.
- **Impact on the Company**: This is assessed based on the potential consequences in terms of financial and prohibitive sanctions resulting from the commission of the crime.
- **Significance of the Crime**: This is evaluated in terms of the advantage it would provide to the company's reality, based on the company's processes, staff competencies, IT systems, machinery, and equipment, categorized into three levels:
  - **Low**: Crimes that, although applicable, would offer little advantage.
  - **Medium**: Crimes that would likely provide some advantage.
  - **High**: Crimes that would undoubtedly provide a significant advantage.
- **Probability of Commission**: This is calculated based on the controls and systems implemented by the Company, proportionally to the company's scale. Examples include:
  - **Delegations/Organizational Structure**: Defined responsibilities through organizational charts, job descriptions, or assignments, delegations, and powers of attorney. The level of formalization must be appropriate not only to the company's reality but also to the nature of the activities and processes involved, especially in health and safety where it is defined by legal norms.
  - **Presence/Suitability of Procedures**: Formalized company provisions (procedures, operational instructions, etc.) related to behavior principles, performance of sensitive activities, and documentation archiving.
  - **Training and Communication**: Aspects concerning employees in general, related to internal organizational provisions (e.g., organizational hierarchy, internal communication flows, specific job procedures). Communication should be thorough, effective, authoritative, clear, detailed, and accessible, whether in paper or digital format. Training must cover both mandatory health and safety aspects and compliance with Legislative Decree 231 provisions, with monitoring of attendance, content quality, and any update needs.
  - **Segregation of Duties**: Separation of activities and responsibilities (see paragraph

4.1).

- **Controls and Traceability of Operations**: Activities that document, even over time, the actions performed (see paragraph 4.2).

The final **risk level** is expressed with a numerical value from 1 to 16, determined by the combination of impact, significance of the crime for the company, and probability of commission, as outlined in the following table:

RISK CALCULATION PARAMETERS	SIGNIFICANCE		0,5 (low)	0,8 (medium)	1 (high)
	PROBABILITY	1	2	3	4
	IMPACT	1	2	3	4

RISK LEVEL	1	2	3	4
	5	6	7	8
	9	10	12	13
	16			

6.4.4. Phase 4: Definition of Special Parts and Procedures

The final phase involves, based on the results from the previous phases, identifying specific prevention measures, which consist of operational instructions to prevent the commission of crimes. For each process where risk activities have been identified, a specific document is created which includes:

- **Crime Categories**: The types of crimes that could affect the process.
- **General Principles Applicable to the Process**: General requirements that must be observed by all individuals involved in sensitive areas.
- **Business Functions Involved**: The company functions responsible for managing sensitive activities.
- **Specific Procedures Applicable to the Process**: Special provisions governing various risk activities/sensitive processes. Each provision must:
  - **Be Defined**: Clearly articulated.
  - **Be Assigned to Specific Functions**: Designated to particular roles or departments.
  - **Be Verifiable**: Documented to ensure internal control, with references to specific company regulations if they exist.
- **Controls by the Supervisory Body**: General principles of control by the Supervisory Body (ODV) over the specific process.

7. Violation Reporting System (Whistleblowing)

Legislative Decree No. 24 of March 16, 2023, enacted to implement EU Directive 2019/1937, regulates the protection of individuals who report crimes or irregularities they become aware of within the scope of an employment relationship, ensuring confidentiality throughout the entire reporting process.

The Decree requires companies with an organizational model (MOG) as per Legislative Decree No. 231 to establish at least **one INTERNAL reporting channel** that ensures the confidentiality of the whistleblower's identity. This channel (known as the **INTERNAL Whistleblowing**) must be managed by specifically trained personnel designated to handle and manage reports. The personnel can be either *internal* (e.g., a function manager or a specific person identified by the company) or *external* (e.g., the Supervisory Body - ODV).

The legislation also provides that reports can be made through **an EXTERNAL channel** (known as the **EXTERNAL Whistleblowing**), with the National Anti-Corruption Authority (ANAC) designated as the body to manage the report under the following conditions:

- The mandatory activation of the internal reporting channel is not provided for within the work context, or the internal channel, although mandatory, is inactive or non-compliant with the regulations.
- The whistleblower has already made an internal report, which has not been followed up or has resulted in a negative final decision.
- The whistleblower has reasonable grounds to believe that an internal report would not be effectively acted upon or could lead to retaliation.
- The whistleblower has reasonable grounds to believe that the violation poses an imminent and apparent danger to the public interest.

Reports to ANAC can be made in writing via the online platform according to ANAC Guidelines, or orally through telephone lines or voice messaging systems, or, upon request by the whistleblower, through a direct meeting arranged within a reasonable time frame.

In any case, the purpose of the whistleblowing system is to protect employees who report crimes or irregularities they become aware of in the course of their work and to foster a "social conscience" within the workplace, encouraging individuals to report any misconduct they encounter during their work duties, either to the authorities or to their employer.

The legislation also provides for:

- Administrative penalties for the company in the case of failure to establish the internal channel;
- Disciplinary penalties for individuals who violate the reporting system;
- Penalties for individuals who engage in retaliatory and intimidating acts against whistleblowers, as described further in this document (see paragraph 8 Disciplinary System).

The following describes the INTERNAL reporting system adopted by the Company, which ensures maximum dissemination and availability:

- **To its staff**, both current and newly hired, through direct distribution and brief training sessions, and publication through internal company channels (intranet, company bulletin board, etc.);
- **To all Recipients** who have a legal relationship with the Company.

The Company is responsible for ensuring the widespread dissemination of information regarding the EXTERNAL reporting channel as well. If the Company has its own website, it publishes the information defined by it in a dedicated section of the site.

7.1. Scope of Application

The reporting system applies to all Recipients of the MOG, including those holding representative, administrative, managerial, or control functions within the Company or its organizational units, as well as individuals subject to the oversight of such persons.

The report, based on good faith or reasonable belief, must concern specific instances of illicit conduct relevant under Legislative Decree No. 231, as well as under national and EU law, and must be based on factual, precise, and consistent elements or violations of the Organization's MOG that the whistleblower has become aware of due to their functions or activities performed.

7.2. Responsibilities of the Receiver

The individual responsible for receiving reports must adhere to confidentiality obligations regarding the information, data, and personal data of the whistleblower, the reported individuals, and the contents of the reports, in full compliance with EU Regulation 2016/679. They must also follow the provisions of the MOG and the Code of Ethics, as well as legal requirements. This person must be appropriately trained and designated as authorized to process personal data (Article 4, No. 10 GDPR and Article 2 quaterdecies of Legislative Decree No. 101/2018).

Failure to comply with confidentiality obligations, particularly regarding the protection of the whistleblower's privacy, will result in dismissal from the role, in addition to the application of disciplinary sanctions as provided by the employment contract and the Company's disciplinary system (see paragraph 8).

Specifically, the individual receiving the report must:

- Ensure the preservation and privacy of the original documentation related to reports in designated physical or digital archives, with appropriate security/confidentiality standards in place.
- Monitor communication channels (regular and registered mail, platforms).
- Evaluate requests for the adoption of organizational measures and/or the imposition of sanctions or disciplinary measures and/or the initiation of legal actions.

If the receiver appointed by the Company is not a member of the ODV, they must promptly forward a copy of the report, including any attachments, to the ODV for its awareness. The transmission of the report must be done in the utmost confidentiality and in a manner that protects the whistleblower and the identity and reputation of the reported individuals, without compromising the effectiveness of subsequent investigative activities.

7.3. Content of the Report and Reporting Methods

The report must be submitted using the *Report Form, M_MOG PG_02*, which requires the inclusion of the following mandatory information:

a) **Whistleblower's Details**: Including the name and position or role held within the Company;
b) **Subject of the Report**: The topic or issue being reported;
c) **Time and Place**: The circumstances of time and place where the reported facts occurred;
d) **Identification of the Perpetrator**: Elements that help identify the person responsible for the reported facts;
e) **Source of Information**: How the information was obtained;
f) **Other Individuals**: Indication of other people who might have information about the reported facts;
g) **Detailed Description**: A clear and complete description of the reported facts, including any supporting documents

necessary for subsequent verification and investigation of the validity of the reported facts.

The report must be submitted through the following methods:

a) **Via Email**: To the recipient's email address, with the username and password known only to the recipient;
b) **By Mail**: Sent by registered post to the Company's legal office addressed to the recipient, with the report placed in a sealed envelope marked as "confidential" or "personal";
c) **Verbally**: Through an oral statement, which must then be documented by the recipient through recording on an appropriate device or via a written report signed by both the recipient and the whistleblower;
d) **Through a Dedicated Platform**: If available, via a dedicated online platform.

7.4. Handling the Report

For each report received, the recipient must:

- **Acknowledge Receipt**: Inform the whistleblower of the receipt of the report within 7 days of receipt.
- **Maintain Communication**: Keep in touch with the whistleblower and request, if necessary, additional information.

- **Respond Diligently**: Follow up on the received report and provide feedback within 3 months from the date of receipt acknowledgment (if no acknowledgment is provided, within 3 months from the expiration of the seven-day period from the submission of the report).
- **Data Privacy Information**: Provide the whistleblower with information about the processing of personal data within 7 days of receipt of the report, in accordance with Articles 13 and 14 of the GDPR.
- **Inform About Procedures**: Provide information on the methods and procedures to be applied to the reports.

7.5. Whistleblower Protection Measures

7.5.1. Confidentiality Obligations Regarding the Whistleblower's Identity

The Company ensures that the information collected related to the report remains confidential, except in the following cases:

- **Whistleblower Consent**: If the whistleblower consents to the disclosure (processing) of their personal data;
- **Legal Requirements**: If required by law (for example, if it is necessary to involve authorities).
- **Health or Safety Protection**: When necessary to safeguard the health or safety of individuals;
- **Essential for Defense**: When it is essential for the defense during the hearing of the accused, for the presentation of defensive statements (the necessity must be justified and demonstrated);
- **Liability for Defamation**: When there is a potential liability for false accusation or defamation.

All individuals who receive or are involved in managing reports are required to protect the confidentiality of such information.

Unauthorized disclosure of the whistleblower's identity or information from which it can be inferred is considered a violation of the MOG (Management and Organization Model).

7.5.2. Disclosure of Information or Discrimination

For reports made in the forms and within the limits described below, the Company provides protection to employees under D. Lgs. 231/2001 in cases of disclosure of information subject to confidentiality obligations, whether it be official, business, professional, scientific, or industrial.

When information and documents communicated to the designated authority are subject to business, professional, or official confidentiality, revealing such information in a manner that exceeds the purpose of eliminating the illicit activity constitutes a breach of confidentiality. Specifically, disclosing

information outside the designated communication channels for this purpose is considered a violation.

The protection does not apply if the confidentiality obligation affects someone who learned of the information due to a professional consultancy or assistance relationship with the Company or if the confidentiality is breached outside the specific communication channels.

7.5.3. Prohibition of Retaliation or Discrimination

"Retaliatory" and/or "discriminatory" measures refer to actions taken against an employee who has made a report, including but not limited to:

- Termination: Dismissal, suspension, or equivalent measures;
- Demotion: Reduction in rank or denial of promotion;
- Change in Duties: Alteration of job functions or work location;
- Training Suspension: Suspension of training or any restriction on access to it;
- Negative Performance Reviews: Receiving negative performance evaluations or references;
- Disciplinary Measures: Adoption of disciplinary measures or other penalties, including financial ones;
- Coercion, intimidation, harassment, or ostracism;
- Discrimination or unfavorable treatment
- Contractual Changes: Failure to convert a fixed-term contract to a permanent contract when there is a legitimate expectation of such a conversion;
- Contract Renewal: Non-renewal or early termination of a fixed-term contract;
- Reputational Damage: Damage to the individual's reputation, especially on social media, or financial or economic prejudice, including loss of economic opportunities and income;
- Improper Listing: Inclusion on inappropriate lists based on formal or informal sectoral or industrial agreements, which may hinder future employment in the sector or industry;
- Supply Contracts: Early termination or cancellation of supply contracts for goods or services;
- Licenses or Permits: Cancellation of a license or permit.
- Request for Psychiatric or Medical Examinations: Any request for psychiatric or medical evaluations.

The Company does not permit or tolerate any form of retaliation or discriminatory measures that affect the working conditions of an employee who makes a report related directly or indirectly to the report.

Additionally, the whistleblower has the right to request a transfer to another office or department, and where reasonably possible, the Company must accommodate such requests.

Protection is limited to cases where both the whistleblower and the accused are employees of the same Company.

Should it be determined that a person has engaged in retaliatory acts as described in Article 17 of D. Lgs. 24/2023 and mentioned above, they will be subject to the following disciplinary sanctions, commensurate with the severity and effects of the conduct:

- Revocation: Removal from their appointment or duties;
- Verbal Warning: A verbal reprimand;
- Written Warning: A written warning;
- Fine/Suspension: A fine or suspension from work not exceeding what is provided by the applicable National Collective Bargaining Agreement (CCNL);
- Non-Disciplinary Suspension: A precautionary suspension not related to disciplinary action;
- Dismissal for Just Cause: Termination of employment for just cause.

Compensation for damages is always reserved.

If an employee believes they have been discriminated against for making a report, they should report the facts to the recipient, who, within the required timeframe, will assess the situation and promptly evaluate:

- the need to adopt measures to restore the situation and/or remedy the negative effects of the discrimination;
- whether there are grounds to initiate disciplinary proceedings against the employee responsible for the discrimination.

Requests for the adoption of organizational measures and/or the imposition of sanctions or disciplinary actions and/or the initiation of legal actions are the responsibility of the Management for approval.

These provisions do not affect the criminal and disciplinary responsibility of the whistleblower in cases of false or defamatory reporting under the Penal Code and Article 2043 of the Civil Code.

Additionally, any abuse of these provisions for the sole purpose of harming the accused or for opportunistic reasons will also be a source of disciplinary and other relevant responsibilities.

8. Sanction System

The provision of a sanctioning and disciplinary system constitutes, pursuant to Article 6, paragraph 1, letter e) of Legislative Decree 231/2001, an essential requirement for exemption from the Company's liability and is a necessary condition to ensure the effectiveness of the MOG (Management and Organization Model) and the efficiency of the Supervisory Board (ODV) action.

This system is independent of other disciplinary infraction procedures and is distinct and separate from the criminal sanctioning system that may result from criminal offenses committed by individuals.

The disciplinary system provides for sanctions for each Recipient of the MOG, considering the different types of relationships, which may be disciplinary in some cases and contractual/negotiable in others.

The application of the disciplinary system and related sanctions is independent of the existence and outcome of any criminal proceedings that may be initiated by the Judicial Authority if the behaviour being censured also constitutes a criminal offense under Legislative Decree 231/2001.

In accordance with Article 7 of the Workers' Statute, this Disciplinary System must be made known to employees through posting in areas of the workplace accessible to all personnel or through dissemination via the company's intranet system.

The sanctioning and disciplinary system also applies in cases of violations of certain company procedures that, although not constituting criminal offenses under Legislative Decree 231/01, are considered relevant due to their technical-organizational, legal, economic, or reputational implications for the Company. Specifically, this includes operational procedures related to reference regulations for the industry in which the Company operates, as well as procedures governing "core" processes as classified by the Company.

In addition to the posting obligations, along with the Code of Ethics, this sanctioning and disciplinary system must be communicated during appropriate informational sessions directed at all Recipients.

Recipients are required to report any violations of this sanctioning and disciplinary system to the recipient of the **INTERNAL reporting channel**, following the procedures described in paragraph *7. Whistleblowing System*.

8.1. Scope of Application

The Sanction and Disciplinary System is primarily framed within the general obligations stipulated by Articles 2104, 2105, 2106, 2118, and 2119 of the Civil Code, concerning the diligence and obedience of the worker, and the employer's powers to implement and enforce specific disciplinary measures, as integrated by the National Collective Labor Agreements (CCNL) and the Workers' Statute.

The system provides for sanctions that are proportional to the severity of the infraction committed and is designed to comply with the provisions of the Workers' Statute and the applicable CCNLs. The potential recipients of disciplinary measures are mainly Senior Management and employees under others' direction. This includes those referred to in Articles 2094 and 2095 of the Civil Code (subordinate workers) and, where no imperative legal norms apply, all stakeholders of the company.

The Sanction and Disciplinary System complements, but does not replace, the general disciplinary system related to the employment relationship as regulated by public and private labour law.

8.2. Responsibility for Application

The company is responsible for formalizing, revising, and applying the Sanction and Disciplinary System.

The Supervisory Body (ODV), as per Articles 6 and 7 of Legislative Decree 231/2001, has the role of overseeing the proper implementation of the MOG, with specific functions of supervision concerning those infractions that might affect the functionality of the MOG. Consequently, in accordance with the Workers' Statute, the ODV must be informed of any application of sanctions and can provide evaluations regarding the events without being bound by terms or decisions for the company function responsible for deciding and imposing the sanction.

8.3. Operational Modalities for applying the Sanction System

The following details the operational modalities for applying the sanction and disciplinary system according to the different types of Recipients and the various disciplinary sanctions.

8.3.1. Employees

Regarding Employees, it is necessary to respect the limits related to the sanctioning power imposed by Article 7 of Law No. 300/1970 (known as the "Workers' Statute") and the relevant CCNL (National Collective Labor Agreement), both in terms of the applicable sanctions, which have already been identified and associated with types of disciplinary violations, and the way this power is exercised.

The Company believes that the currently applied Sanction and Disciplinary System, in line with the provisions of the relevant CCNL (National Collective Labor Agreement), meets the required standards of effectiveness and deterrence.

The following constitute a breach of the obligations deriving from the employment relationship and disciplinary misconduct:

- Failure to comply with or violation of the general principles of the MOG.
- Failure to comply with or violation of the principles expressed in the company's Code of Ethics.
- Failure to comply with or violation of the provisions contained in the Protocols (procedures, regulations, etc.).
- Making unfounded reports with intent or gross negligence.
- Violation of measures to protect the confidentiality of the reporter.

The prescribed sanctions are adopted and applied in compliance with the procedures provided by national and company collective labour agreements relevant to the ongoing employment relationship.

The following table lists the sanctions provided by the CCNL (National Collective Labor Agreement) and some examples (not exhaustive and for illustrative purposes only).

Sanction Type (provided for by the CCNL)	Case Studies
A) VERBAL WARNING	▪ minor non-compliance with the rules of conduct of the Company ▪ Code of Ethics and the protocols provided for by the Model ▪ minor non-compliance with the Company Procedures and/or the ▪ Internal Control System carried out by the Supervisory Body (hereinafter, also the "Internal Control System") ▪ tolerance of minor non-compliance or irregularities committed by one's subordinates or other members of the staff pursuant to the Model, the protocols, the Internal Control System and the Company Procedures ▪ failure to comply due to minor negligence with requests for information or the presentation of documents by the Supervisory Body, except for reasonable justifications
NOTE: there is "***slight non-compliance***" in cases where the conduct is not characterized by malice or gross negligence and has not generated risks of sanctions or damages for the Company. **NOTE**: in the event that the behaviour is such as to expose the Company to a risk of crime relating to the family of crimes *25septies – "Crimes of manslaughter and serious or very serious negligent injury, committed in violation of the accident prevention and health and hygiene protection at work regulations"*, the warning must still be written.	
B) WRITTEN WARNING	▪ culpable failure to comply with the rules of conduct of the Company Code of Ethics and the protocols provided for by the Model. ▪ culpable failure to comply with Company Procedures and/or the Internal Control System. ▪ tolerance of culpable failure to comply by subordinates or by other members of the staff pursuant to the Model, the protocols, the Internal Control System and Company Procedures. ▪ failure to comply with requests for information or to show documents by the Supervisory Body, except for motivated justifications.
NOTE: there is "***culpable failure to comply***" in cases where the conduct is not characterised by intent or has generated potential risks of sanctions or damages for the Company	
C) FINE / SUSPENSION FROM WORK (not exceeding what is provided by the terms of the applicable CCNL)	▪ non-compliance punishable by the previous sanctions, when, due to objective circumstances, specific consequences or recidivism, they are of greater importance. ▪ repeated or serious non-compliance with the rules of conduct of the Company Code of Ethics and the protocols provided for by the MOG. ▪ repeated or serious non-compliance with company procedures and/or the Internal Control System. ▪ failure to report or tolerate serious non-compliance committed by subordinates or other members of the staff pursuant to the MOG, the Protocols, the Internal Control System and the Company Procedures. ▪ repeated failure to comply with requests for information or the exhibition of documents by the Supervisory Body (ODV), except for motivated justifications.

NOTE: in the event that the behaviour is such as to expose the Company to a risk of crime relating to the family of crimes 25-septies – "Crimes of manslaughter and serious or very serious negligent injury, committed in violation of the accident prevention and health and hygiene at work regulations", the fine will be increased by 20% of the amount estimated for an exposure to the same risk committed in other families of crimes. The amount of the fines will be donated to any of the social institutions in favour of workers.	
D) PRECAUTIONARY SUSPENSION (Non-Disciplinary)	▪ This measure is applied to employees under preliminary investigation or subject to criminal proceedings. The Company may decide, at any stage of the ongoing criminal proceedings, to temporarily remove the individual from service for precautionary reasons.
NOTE: In cases where the preliminary investigation or criminal proceedings concern a crime related to the category of crimes under 25-septies – "Crimes of manslaughter and serious or very serious negligent injury, committed in violation of the accident prevention and health and hygiene at work regulations", the period of removal from service will be increased by 20% compared to the duration established for exposure to risk for similar acts under other crime categories. The removal from service must be communicated in writing to the employee concerned and may be maintained by the Company for as long as deemed necessary, but not beyond the point when the criminal court's decision becomes final. An employee removed from service retains the right to their full compensation during this period, and the time is considered as active service for all other purposes as provided by the applicable National Collective Labor Agreement (CCNL).	
E) DISMISSAL FOR JUST CAUSE	▪ deliberate breach of company regulations issued under Legislative Decree 231/2001, of such severity—whether due to the intentional nature of the act, its criminal or financial implications, recidivism, or its particular nature—as to undermine the trust upon which the employment relationship is based, and which prevents the continuation of the employment relationship, even on a provisional basis. ▪ deliberate performance of acts not required or omission of acts required under the MOG or its related Protocols, which has resulted, following a judicial process, in the Company being sentenced to monetary and/or disqualifying penalties for having committed the crimes provided for by Legislative Decree 231/2001. ▪ deliberate breach of company procedures of such gravity—due to the intentional nature of the act, its technical-organizational, legal, economic, or reputational implications, or recidivism, or its particular nature—as to undermine the trust upon which the employment relationship is based, and which prevents the continuation of the relationship, even on a provisional basis.
NOTE: A **significant breach (whether deliberate or with gross negligence)** of the behavioural rules provided by the MOG, the Code of Ethics, the related protocols, and the Company Procedures, which causes serious moral or material harm to the Company and does not allow the continuation of the relationship even on a temporary basis, is considered a serious violation. This includes the adoption of behaviours that constitute one or more crimes or unlawful acts that form the basis of the Crimes.	

8.3.2. Directors

The Administrative Body is the designated function to take appropriate action in the case of:

- Commission of crimes or violation of the Code of Ethics, the MOG, and/or related Protocols by Directors;
- False reports made with deliberate misconduct or gross negligence;
- Violation of measures to protect the confidentiality of the whistleblower.

In cases of serious violations by Directors, the act may be considered just cause for the revocation of the Director by the Shareholders' Meeting.

Note: A ***serious violation*** is considered to be the commission of crimes understood as the conduct constituting the Crimes. If applicable, the Company may take action to claim damages.

8.3.3. Members of the Supervisory Body (ODV)

The Administrative Body is the designated function to take appropriate action in the case of the commission of crimes or violation of the Code of Ethics, the MOG, and/or related Protocols by members of the Supervisory Body (ODV).

In cases of serious violations that are not justified and/or not ratified by the Administrative Body, the act may be considered just cause for the revocation of the assignment, without prejudice to the application of disciplinary sanctions provided for in existing contracts (employment, supply, etc.).

8.3.4. Suppliers or Other Parties

Where possible, a necessary condition for validly concluding contracts of any type with the Company, particularly supply and consultancy contracts, is the third-party contractor's commitment to comply with the Code of Ethics and/or the Protocols applicable in relation to the services covered by the contract.

Such contracts, where possible, include termination clauses or withdrawal rights in favour of the Company without any penalty for the latter, in the event of the commission of Crimes or conduct constituting the Crimes, or in the case of violation of the rules of the Code of Ethics, the MOG, and/or related Protocols, including those related to reporting procedures, and particularly in the case of non-compliance with safety requirements.

In any case, the commission of illegal acts or behaviours that violate the Company's Code of Ethics or Protocols will be considered just cause for the termination of the contract pursuant to Articles 1453 et seq. of the Civil Code.

The document "*List of Example Contract Clauses, A_MOG PG_02*" lists some examples of contract clauses significant for the Company.

The Company reserves the right to take criminal action and to seek damages if such behaviour causes any kind of damage to the Company, such as in the case of the judge's application of the

measures provided for by the Decree.

8.3.5. Self-employed Workers and Collaborators of the Company

With regard to self-employed workers and collaborators of the Company, violations or circumvention of the MOG, the Code of Ethics, and/or protocols, as well as the making of false reports with deliberate misconduct or gross negligence, or the violation of measures to protect the confidentiality of the whistleblower, represent a serious breach in the execution of contracts. Therefore, the provisions of Article 1453 et seq. of the Civil Code regarding the termination of the contract for non-performance apply.

Consequently, in all relations with such parties, where possible, specific termination clauses must be included in supply and collaboration contracts, as well as clauses for damage compensation and indemnification.

The Company reserves the right to take criminal action and to seek damages if such behaviour causes any kind of damage to the Company, such as in the case of the judge's application of the measures provided for by the Decree.