ORGANIZATION, MANAGEMENT AND CONTROL MODEL

Legislative Decree no. 231 of 8 June 2001

Issue 14 of October 23, 2026

Summary

1.	**Definitions**	**3**
2.	**Introduction**	**7**
3.	**Summary of the Decree and Relevant Legislation**	**8**
4.	**Function and adoption of the Organizational Model**	**12**
5.	**AC BOILERS**	**14**
5.1	**The Company**	**14**
5.2	**Type of business and market/Customers**	**14**
5.3	**Investments**	**14**
6.	**The Organizational System**	**15**
6.1	**The Organizational System**	**15**
6.2	**Delegation of powers: ordering principles and purposes**	**15**
6.3	**Flowchart**	**16**
6.4	**Supervisory Body (SB)**	**17**
6.4.1	**Reporting by the Supervisory Body**	**18**
6.4.2	**Information flows to the Supervisory Body**	**18**
6.4.3	**Whistleblowing**	**20**
7.	**Use of artificial intelligence systems**	**21**
8.	**Sustainability governance and ESG risk management**	**21**
8.1	**Sustainable supply chain and CBAM**	**21**
9.	**Disciplinary System**	**22**
9.1	**General principles**	**22**
9.2	**Penalties against employees**	**22**
9.3	**Measures against Managers**	**23**
9.4	**Measures against Directors and Statutory Auditors**	**23**
9.5	**Measures against Consultants and Partners**	**23**
9.6	**Measures applicable to the recipients of reports ("Whistleblowing")**	**23**
10.	**Mapping of potential risks of predicate offences**	**24**
11.	**Update of the Organizational Model**	**25**
12.	**Reference documents for the preparation of the Organisational Model**	**25**
13.	**Annexes to the Organisational Model**	**25**
Appendix: Evolution of the Organizational Model		**26**

1. DEFINITIONS

***Corporate Governance (CG)*:** The *Corporate Governance* or Internal Control System is the set of rules, at each level (laws, regulations, company procedures, etc.) which governs the management of the company itself. The CG also includes the relationships between the various parties involved (the *stakeholders*) and the objectives for which the undertaking is managed. The main *Actors* are the Shareholders, the management and the Board of Directors.

Sensitive Activity: Phase of a process in which activities at risk of committing a crime have been identified.

Code of Ethics (CE): The CE is a code of conduct adopted in the performance of its activities and business. The Code adopts – as reference directives – the laws, regulations and internal protocols of the Company. The EC therefore establishes – for all its employees, directors, corporate bodies, collaborators, suppliers, etc. – the fundamental rules of conduct based on ethical principles of correctness, loyalty, transparency, honesty and confidentiality and on respect for and protection of the environment, as well as the health and safety of workers and the community in which the Company operates.

Supplier Code of Conduct: This is the documented standards of companies for the members of their supply chain ecosystems, as well as a useful tool to ensure that suppliers, subcontractors and subsidiaries share their values in relation to labour standards, health and safety, environmental impacts and business ethics.

***Compliance*:** It is the compliance of company activities with legislative provisions, standards, regulations, procedures and codes of conduct. *Corporate compliance* is therefore a preventive activity that is concerned with preventing the risk of non-compliance of the company's activities with the mandatory rules and laws, suggesting – where misalignments are found – the most appropriate corrections.

Consultants: Persons who act in the name and/or on behalf of the Company, by virtue of a professional collaboration contract.

Employees: Employees of the Company whose relationship is regulated by a fixed-term or permanent employment contract.

Legislative Decree 231/2001: Legislative Decree 231 of 2001 establishes the administrative liability of Entities for crimes committed by directors, managers and/or employees in the interest or to the advantage of the Entities themselves.
It is therefore aimed at: Entities with legal personality, companies with legal personality and associations, including those without legal personality. Exceptions are the State, local public bodies and bodies with functions of constitutional importance. The liability of the company is excluded if the natural person has committed the crime for his or her own exclusive benefit or that of third parties. The Decree also provided that each company may avoid an administrative offence by adopting and enforcing its own "Organisation, Management and Control Model" (Organisational Model) and by establishing a Supervisory Body that effectively implements controls on compliance with the Model.

Legal person: It means an organized complex of people and goods to which the legal system attributes the legal capacity (the attitude of a subject to be the holder of rights and duties) thus making it a legal subject.

Entity: Identify the Legal Company and also private organizations that have not obtained recognition and are therefore not, in fact, legal persons (the so-called de facto entities, such as political parties and trade unions).
The same applies to public organizations without legal personality but part of a larger Public Body, to which the law recognizes a certain autonomy. When the legal system attributes to entities, even if they do not have legal personality, a certain degree of patrimonial autonomy, according to a widespread theory, they can still be considered subjects of law.

Types of crimes: Types of crimes identified by Legislative Decree 231/2001 and subsequent additions and/or amendments that "do not apply to the State, local public bodies, other non-economic public bodies as well as bodies that perform functions of constitutional importance".

Insider Trading: An Anglo-Saxon term indicating the illicit practice of using confidential information or information not yet disclosed to the market in order to carry out speculative operations on the stock exchange and, therefore, make illicit profits in the purchase and sale of securities. Insider trading is prohibited and is governed by Law 157/1992 and subsequent additions or updates.

Guidelines (LG): The Confindustria Guidelines provide the Guidelines that a company can follow for the construction of its Model. The LGs are approved in advance by the Ministry of Justice. The first edition of the LG was released on March 7, 2002.

Organizational Model (MO): The "Organizational Model" provides:
- a Code of Ethics, as a code of conduct adopted by the Company which, by listing the ethical principles, serves as a premise for the Model;
- a company organization chart with the identification of the Management and the subjects in top positions, the others being subject to the direction of others (employees and collaborators);
- a risk analysis (through process mapping and analysis of individual risk areas, with the identification of positions and functions that direct the business activity);
- a formulation of binding company directives (procedures that identify activities, responsibilities and related controls);
- the identification of a Supervisory Body (SB) that supervises the application of the Model;
- the identification and planning of preventive control methods (audit plans);
- the identification of a disciplinary system for non-compliance with the CE and the Model.

OHSAS 18001: Standard that supports companies in formulating objectives and policies in favour of Occupational Health and Safety (OSH), according to the provisions of current regulations and based on the hazards and risks potentially present in the workplace.

Corporate bodies: Board of Directors, Board of Statutory Auditors.

Supervisory Body (SB): Body of a company, appointed by the Board of Directors, and endowed with powers of initiative and control, which is entrusted with the task of supervising the functioning and compliance with the CE and the Model and of taking care of their updating and dissemination (pursuant to Legislative Decree 231/2001 and LG).

Special Section: In-depth guide, part of the Organisational Model, on the offences envisaged by Legislative Decree 231/2001 and on the company areas at potential risk.

Personnel: Employees, members of the Board of Directors, members of the Board of Statutory Auditors, members of the Supervisory Body.

Attorneys: Persons to whom the Company has conferred powers for management purposes; they enter into commitments with third parties on behalf of the Company.

Public Administration (PA): The Public Administration made up of public bodies, private concessionaires of public services, public companies and bodies governed by public law that are called upon to operate, in relation to the area of activity considered, in the exercise of a public function.

Public official (Article 357 of the Italian Criminal Code): public officials are those who exercise a legislative, judicial or administrative public function. For the same purposes, the administrative function governed by rules of public law and by authorization acts, and characterized by the formation and manifestation of the will of the public administration or by its performance by means of authorization or certification powers, is public. In a broad sense, the notion of Public Entity and Public Official also includes entities (and consequently the persons who are part of it) that perform public utility services (Enel, Telecom, Municipal Companies, etc.), even if regulated by private law rules.

Crimes: Types of crimes contemplated in Legislative Decree 231/2001 and subsequent additions.

EC Reg. 761/01 EMAS: This is the acronym for *Environmental Management and Audit Scheme*, i.e. "Environmental Eco-Management and Eco-Audit System".

Risk(s): The combination of the probability of an event and its consequences. Business processes are aimed at managing risks in an integrated way and their analysis must be, as far as possible, referred to a general model of business risks that must be detailed and customized to the specific business reality. In general, the most recurrent risks can be classified into management risks (contractual commitments, etc.), strategic risks (organizational structure, joint ventures, alliances, etc.), financial risks (tax management, money laundering, payments, etc.) and external risks (laws and regulations, competition, etc.).

SA 8000: The SA 8000 standard (*Social Accountability*) is an international standard, developed in 1997 by the American body SAI, which contains the social requirements of those organizations that voluntarily provide a guarantee of ethics of their 'production chain' and their production cycle. SA 8000 is based on ILO conventions, the Universal Declaration of Human Rights, and United Nations Conventions.

Top Managers: Persons who hold the functions of representation, administration and management of the Company or of one of its organisational units with financial and functional autonomy, as well as by persons who exercise, even de facto, the management and control of the same.

Stakeholders: These are all those "stakeholders" who work in concert with the Company. These include Shareholders, Employees and Collaborators, Customers, Suppliers, Partners, Lenders, Competitors, the State with its Public Administrations and the community in the broadest sense.

UNI EN ISO 14001: The standard is an international instrument that specifies the requirements of an environmental management system. It is issued by an accredited independent body that verifies the concrete commitment to minimizing the environmental impact of processes, products and services, certifying with the ISO 14001 mark the reliability of the EMS (Environmental Management System) applied.

2. INTRODUCTION

In 2004 AC Boilers S.p.A. (formerly Ansaldo Caldaie S.p.A.) voluntarily adhered to the provisions of Legislative Decree 231 of 8 June 2001 by adopting the Code of Ethics and the Organisational Management and Control Model.
In 2008, the Model was extensively revised both to incorporate further legislation and to be adapted to AC Boilers's organisational developments, also pursuing the objective of incisively strengthening the governance system, subjecting the identification of areas of potential risk to careful verification in advance.
Over the years, the Model has been updated with the introduction of the new offences provided for by Regulation 231 and with the changes to the corporate organisational structure adopted by the Company.
The Organisational Model consists of a General Part, which defines the criteria and lines of method subsequently developed in the Special Part by type of offence and in the related Protocols, aimed at regulating the performance of risky activities, as well as the rules aimed at planning the formation of decisions in relation to the individual offences to be prevented.

AC Boilers undertakes to promptly update the Model in the event that inadequacies – even if only partial – are highlighted such as to jeopardise effective risk prevention, or if appreciable changes or modifications occur to the relevant legislative and regulatory system, corporate structure and organisation of the Company.

The task of supervising the operation and compliance with the aforementioned Model and of ensuring that it is updated has been entrusted to a Supervisory Body, appointed by the Board of Directors, whose composition is promptly communicated after the appointment.

The Managing Director

3. SUMMARY OF THE DECREE AND RELEVANT LEGISLATION

Legislative Decree no. 231 of 8 June 2001 introduced into the Italian legal system a regime of administrative liability (substantially comparable to criminal liability) for legal persons, which is in addition to the liability of the natural person who materially committed the crimes and which aims to involve legal persons (Companies and Entities) in the sanctions.
The administrative liability of the Entity for the commission of one of the crimes provided for by the Decree is in addition to, and does not replace, that (criminal or administrative) of the natural person who is the perpetrator of the offence. The liability of the Entity exists even if the offender has not been identified or the offense itself is extinguished against the offender for a cause other than amnesty.
The Entity cannot be held liable for the commission of any act constituting a crime, but only for the commission of crimes and administrative offences exhaustively provided for by the decree, in the wording resulting from its original text and subsequent additions, as well as from the laws that expressly refer to it.
The liability of the Entity arises if the unlawful act has been committed in the interest of the Entity or to favour the Entity, without the actual and concrete achievement of the objective being in any way necessary.
The offence must also have been committed by one or more qualified persons, belonging to one of the following categories:

- the so-called *"Top management",* persons who hold representation, administration or management functions of the entity or of one of its organisational units with financial and functional autonomy, such as, for example, the legal representative, the administrator, the general manager or the director of a headquarters or branch;
- the so-called "*Subordinates*", persons subject to the direction or supervision of one of the top management who, it should be noted, may not even coincide with the employees.

For offences committed by persons in a "top" position, a rebuttable presumption of liability of the Entity is established, since its liability is excluded only if it proves that – prior to the commission of the offence – it adopted and effectively implemented an Organisation, Management and Control Model and a series of specific measures suitable for preventing the commission of offences of the kind that was committed.
For crimes committed by persons in a "subordinate" position, the Entity can be called upon to answer only if it is ascertained that "the commission of the crime was made possible by the failure to comply with the obligations of management or supervision".

The predicate offences contemplated by the Decree are the following:
Art. 24: *"Undue receipt of disbursements, fraud to the detriment of the State, a public body or the European Union or to obtain public disbursements, IT fraud to the detriment of the State or a public body and fraud in public supplies"* [article amended by Law 161/2017 and Legislative Decree no. 75/2020];
Art. 24-bis: *"IT crimes and unlawful processing of data"* [article added by Law no. 48/2008; amended by Legislative Decree no. 7 and 8/2016, Law Decree no. 105/2019 and Law no. 90 of 28 June 2024];
Article 24-ter: *"Crimes of organized crime"* [article added by Law no. 94/2009 and amended by Law 69/2015];
Art. 25: *"Embezzlement, undue use of money or movable property, bribery, undue inducement to give or promise benefits, corruption"* [amended by Law no. 190/2012, Law 3/2019 and Legislative Decree no. 75/2020. Amended, together with the text, by conversion law no. 112 of 8 August 2024];

Article 25-bis: *"Counterfeiting of coins, public credit cards, revenue stamps and identification instruments or signs"* [article added by Law Decree no. 350/2001, converted with amendments by Law no. 409/2001; amended by Law no. 99/2009; amended by Legislative Decree 125/2016];
Article 25-bis-1: *"Crimes against industry and commerce"* [article added by Law no. 99/2009];
Art. 25-ter: *"Corporate crimes"* [article added by Legislative Decree No. 61/2002, amended by Law No. 190/2012, Law No. 69/2015, Legislative Decree no. 38/2017 and Legislative Decree no. 19 of 2 March 2023];
Article 25-quarter: *"Offences with the purpose of terrorism or subversion of the democratic order provided for by the penal code and special laws"* [article added by Law no. 7/2003];
Article 25-quarter-1: *"Practices of mutilation of female genital organs"* [article added by Law no. 7/2006];
Art. 25-quinquies: *"Crimes against the individual personality"* [article added by Law no. 228/2003; amended by Law no. 199/2016];
Article 25-sexies: *"Crimes of Market Abuse"* [article added by Law no. 62/2005];
"Other cases of market abuse" (Art. 187-quinquies TUF) [article amended by Legislative Decree no. 107/2018];
Art. 25-septies: *"Manslaughter and serious or very serious culpable injuries, committed in violation of accident prevention regulations and on the protection of hygiene and health at work"* [article added by Law no. 123/2007; amended by Law no. 3/2018];
Article 25-octies: *"Receiving stolen goods, laundering and use of money, goods or utilities of illegal origin, as well as self-laundering"* [article added by Legislative Decree no. 231/2007; amended by Law no. 186/2014 and by Legislative Decree no. 195 of 8 November 2021];
Article 25-octies 1: *"Offences relating to means of payment other than cash and fraudulent transfer of values"* [article added by Legislative Decree 184/2021 and amended by Legislative Decree No. 105 of 10 August 2023];
Art. 25-octies 2: "Crimes relating to the violation of restrictive measures of the European Union [article added by Legislative Decree no. 211 of 30 December 2025];
Art. 25-novies: *"Offences relating to copyright infringement"* [article added by Law no. 99/2009];
Article 25-decies: *"Inducement not to make declarations or to make false declarations to the judicial authority"* [article added by Law no. 116/2009];
Art. 25-undecies: *"Environmental Crimes"* [article added by Legislative Decree No. 121/2011, amended by Law No. 68/2015, amended by Legislative Decree no. 21/2018];
Article 25-duodecies: *"Employment of illegally staying third-country nationals"* [article added by Legislative Decree No. 109/2012, amended by Law No. 161 of 17 October 2017];
Art. 25-terdecies: *"Racism and xenophobia"* [article added by Law no. 167 of 20 November 2017, amended by D. Legislative Decree no. 21/2018];
Article 25-quaterdecies: *"Fraud in sports competitions, abusive exercise of gaming or betting and games of chance exercised by means of prohibited machines"* [article added by Law no. 39/2019];
Article 25-quinquiesdecies: *"Tax crimes"* [article added by Law no. 157/2019, by Legislative Decree no. 75/2020 and Legislative Decree 156/22];
Art. 25-sexiesdecies: *"Smuggling"* [article added by Legislative Decree no. 75/2020 and amended in the text by Legislative Decree 141/24];
Art. 25-septiesdecies: *"Crimes against cultural heritage"* [Law no. 22 of 9 March 2022];
Art. 25-duodevicies: *"Laundering of cultural property and devastation and looting of cultural and landscape property"* [Law no. 22 of 9 March 2022];
Article 25-undevicies: *"Provisions regarding Crimes against Animals"* – [Article added by Law no. 82 of 6 June 2025];

Art. 25-vicies: *"Crimes committed using artificial intelligence"* [Article added by Legislative Decree no. 160 of 9 September 2026];
Art. 26: *"Attempted crimes"*;
Law no. 9 of 2013, art. 12:*"Liability of entities for administrative offences dependent on crime"* [They are a prerequisite for entities operating in the virgin olive oil supply chain];
Law no. 146 of 16 March 2006: *"Transnational crimes"* [The following crimes are a prerequisite for the administrative liability of entities if committed in a transnational manner].

The above offences have been included in the Special Section, which is an integral part of the Model.
The Entity can be considered responsible, in Italy, for the commission abroad of certain crimes, provided that the authorities of the State of the place where the act was committed do not proceed against it.
In order to ensure an "effective, proportionate and dissuasive" sanctioning instrument, the legislator has established two main types of sanctions: monetary and disqualification.
The monetary sanction is determined by the judge through a "quota" system. Each offense provides for a minimum and maximum quota based on the seriousness of the offense, the monetary value of which is then determined by the judge, taking into account the "entity's economic and financial conditions", so to ensure the effectiveness of the sanction.
The quota system remains the traditional mechanism, but since 2026, an innovative calculation method based on percentages of the entity's global turnover has been introduced for certain types of offenses.
The proportional method (1%–5% of global turnover) was introduced by Legislative Decree 211/2025 for offenses related to violations of EU restrictive measures.
Disqualification sanctions apply **in addition** to monetary sanctions. They are applied in the most serious cases and can compromise the operational continuity of the organization.
They can last from three months to two years, barring specific aggravating circumstances. They can be temporary or permanent and can also be applied as a precautionary measure. They may include:

1. temporary or permanent prohibition from carrying out the activity;
2. the suspension or revocation of authorisations, licences or concessions functional to the commission of the offence;
3. the prohibition of contracting with the public administration, except to obtain the performance of a public service;
4. the exclusion from facilitations, financing, contributions or subsidies and the possible revocation of those already granted;
5. the temporary or permanent prohibition of advertising goods or services.

In addition to monetary penalties and disqualification sanctions, there are two other sanctions:

- confiscation, which consists in the acquisition by the State of the price or profit of the crime;
- the publication of the sentence of conviction at the expense of the Entity.

The Company may be exempt from administrative liability (Articles 6 and 7 of the Decree) if:

- the subject has acted in his or her own exclusive interest or in the interest of third parties (therefore not in the interest of the Company)

or

1. the management body has adopted and effectively implemented, before the commission of the act, organisational, management and control models suitable for preventing the commission of offences;
2. the task of supervising the operation and compliance of the models and of updating them has been entrusted to a Supervisory Body appointed by the Company, with autonomous powers of

initiative and control;

3. the persons committed the crime by fraudulently circumventing the organization, management and control models;
4. there was no omission (or insufficient) supervision by the Supervisory Body.

The Company must therefore have adopted and effectively implemented organizational, management and control models suitable for preventing the offences from being committed.

These models, in order to be suitable for preventing the risk of offences being committed, must meet the following requirements:

- identify the activities in the context of which the offences may be committed;
- provide for specific protocols, i.e. organisational-procedural elements, aimed at planning the formation and implementation of the Company's decisions in relation to the offences to be prevented (system of powers and delegations, authorisation procedures, operating procedures);
- identify methods of managing financial resources suitable for preventing the commission of crimes;
- provide for the information obligations towards the Supervisory Body;
- adopt a disciplinary system suitable for sanctioning non-compliance with the measures adopted by the Organisation, Management and Control Model.

The scope of application of the sanctioning system provided for by Legislative Decree 231/2001 also applies in the event that the offence has remained at the level of an attempt (Article 26 of the Decree). In fact, the liability of the company can also occur if the predicate crime takes the form of an attempt, i.e. when the acting party performs acts that are unequivocally suitable for committing the crime and the action is not carried out or the event does not occur (Article 56 of the Italian Criminal Code).

In this case, the financial penalties and disqualification are reduced from one third to one-half. Furthermore, the entity is not liable when it voluntarily prevents the performance of the action or the realization of the event.

4. FUNCTION AND ADOPTION OF THE ORGANIZATIONAL MODEL

The Company intends to operate according to ethical principles aimed at shaping the performance of the business, the pursuit of the corporate purpose and the growth of the Company and the Group in compliance with the laws in force.
To this end, it has adopted a Group Code of Ethics, aimed at defining the principles of business ethics that the Company recognizes as its own and requires compliance, and a Supplier Code of Conduct, which outlines the basic expectations for the commercial conduct of suppliers in relation to labour and human rights, health and safety, environmental protection, laws and ethics. The Company is also sensitive to the expectations of its shareholders in terms of fairness and transparency in the conduct of business and is aware, in order to ensure these conditions, of the opportunity to integrate into its internal control system, an organization, management and control model for the prevention of crimes, bearing in mind the provisions of the Decree and the Guidelines drawn up by Confindustria.
This initiative, together with the adoption of the Code of Ethics and the Supplier Code of Conduct, was undertaken in the belief that it can be a valid tool for raising awareness among all the Company's employees and all other parties involved in it (Customers, Suppliers, Partners, external collaborators, etc.), so that they are followed correct and linear behaviours such as to prevent the risk of committing the crimes contemplated in the Decree.
Through the Organisational Model, the Company aims to pursue the following main purposes:

1. prevent the risk of committing crimes;
2. raise awareness among those who work in the name and on behalf of the Company so that every activity is characterised by principles of transparency, fairness and compliance with procedures (internal control);
3. to spread awareness of the risk of incurring, in the event of violation of the provisions contained therein, in disciplinary infractions adequately sanctioned;
4. reiterate that the Company considers any conduct contrary to legal provisions and the ethical principles to which the Company is inspired inadmissible.

The key points of the Organizational Model are:

- the identification of the areas/processes of possible potential risk of committing crimes in the company's activities;
- the definition of an internal regulatory system aimed at planning the formation and implementation of the Company's decisions in relation to the risks/crimes to be prevented through:
  - a Code of Ethics, which sets out the principles and values of the Company;
  - a Supplier Code of Conduct, which helps the Company ensure that suppliers, subcontractors and subsidiaries share their values in relation to labour standards, health and safety, environmental impacts and business ethics;
  - a system of delegation of functions and powers of attorney for the signing of company deeds that ensures a clear and transparent representation of the process of formation and implementation of decisions;
- the determination of a coherent organisational structure aimed at inspiring and controlling the correctness of behaviour, ensuring a clear and organic assignment of tasks and applying a fair segregation of functions;
- the identification of the management and control processes of financial resources in activities at risk of crime;

- the assignment to the SB of the task of supervising the operation and compliance with the Organisational Model and proposing its updating;
- pursuant to the Decree – articles 6 and 7 – the construction of a Disciplinary System for the violation of the rules of conduct of the Code of Ethics and the Model regardless of criminal proceedings.

The Company has chosen to structure its Organisational Model with a first part where legislative references are recalled, a second part that identifies the Company in terms of corporate structure and organisation adopted, a third part where the essential components of the Organisational Model are illustrated with particular reference to the Supervisory Body, staff training and dissemination of the Organisational Model in the corporate context, the disciplinary system as well as the identified risk areas and finally a last part where the possible crimes that can be committed in the company are analysed.

The Organisational Model is associated with the protocols that define the rules, procedures or operational prescriptions adopted for each individual type of offence.

5. AC BOILERS

5.1 The Company

The Company operates directly, including through partnerships, in the reference markets. The Company's bylaws list in detail the activities that constitute the corporate purpose, all in compliance with the provisions, limitations and prohibitions provided for and established by the legislative and implementing provisions in force from time to time. It can also operate with its Customers through Temporary Business Groupings, Joint Ventures, Collaboration Agreements, Consortia and other forms of partnership. To the extent of its competence, the Company undertakes to apply this Model to such Entities and to communicate it to its Partners.

5.2 Type of business and market/Customers

The Company's *products* are mainly: power boilers, biomass and waste to energy boilers, process recovery boilers and service and spare parts.
The *markets* are mainly: Italy and Europe, South America, North Africa and the Middle/Far East.
The *Customers* are mainly: power generation companies, EPC (Engineering Procurement Construction) companies, IPP (Independent Power Producers) companies, public bodies, municipal and state-owned companies, plant manufacturers.

5.3 Investments

RTIs, JVs and other collaboration agreements are not represented as they are linked to the execution of individual orders or projects, or as they are temporary and/or without legal personality; branches, permanent establishments and tax representatives are also not represented as they are a direct emanation of the Company and/or without legal personality.

Investments:
CCA S.p.A. (40% owned) has as its corporate purpose the promotion and performance of research activities and specialist services dedicated to the basic and applied development of its own and third-party products and technological innovations, including through the creation of prototypes and the industrialization of products, on its own behalf and on behalf of third parties.
ANSALDOCALDAIE BOILERS INDIA PV. LTD. (26% owned) operates directly and autonomously on the Indian energy market, with the aim of providing executive engineering, procurement and production activities at competitive costs for AC Boilers projects both on the Indian market and on the Middle and Far East markets.
ITEA S.p.A. (12% owned) has as its corporate purpose the research, study, design, construction, marketing, rental and management of innovative technologies in the environmental sector and of technological systems and components for the recovery and disposal of waste, atmospheric purification, land reclamation and recovery and the remediation of landfills (managed by the company itself or entrusted to others).

6. THE ORGANIZATIONAL SYSTEM

6.1 The Organizational System

The company organisational system identifies and defines the positions, tasks and responsibilities of the company functions, establishing the attributions of responsibility and the hierarchical and functional lines of connection (where necessary) between each sector and each level of the Company. The company organisational system is represented by the company organisation chart shown below, the description of which is reported in the Quality System.

For the purposes of the effectiveness of this Model, it is the Company's specific objective to ensure extensive and correct dissemination of the Code of Ethics, the Supplier Code of Conduct, and knowledge to all employees of the regulations relating to Legislative Decree 231/01 and the Organisational Model and Procedures adopted, as well as their updates over time; to this end, training meetings are periodically scheduled in accordance with the specific procedure.

Employees are therefore required to know and observe the content of both the Code of Ethics and the Organisational Model and to contribute to its concrete implementation and effective functioning.

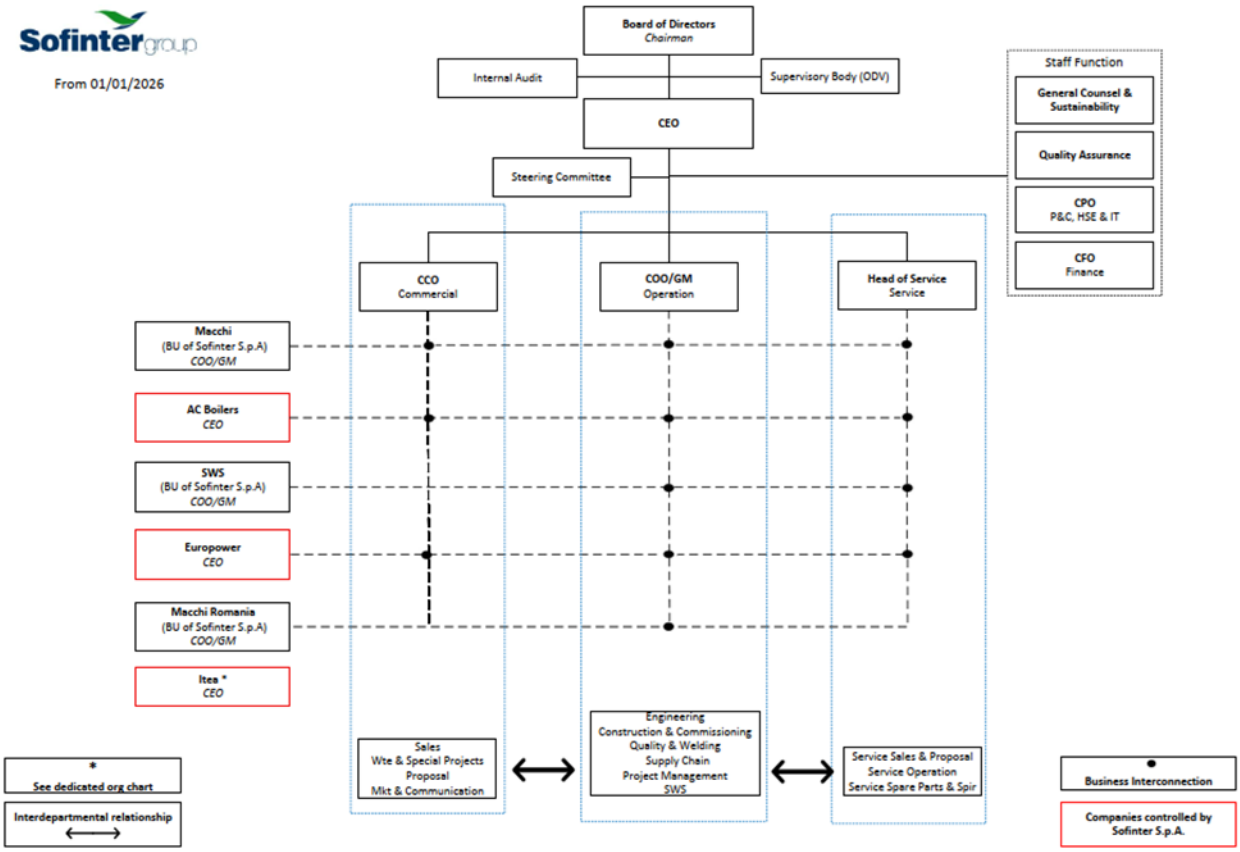
6.2 Delegation of powers: ordering principles and purposes

The system of powers and delegations takes into account the principles dictated by Legislative Decree 231/01 such as:

- The separation of functions;
- The clear identification of the responsibilities assigned;
- The lines of hierarchical subordination;
- Need for territorial supervision;
- The assignment of authorization and signing powers for predetermined values (amounts and conditions).

The powers and delegations assigned are limited to management managers, technical directors and company safety managers.

6.3 Flowchart



The organizational structure of the Company, and more generally of the Sofinter Group, has undergone an optimization process with the aim of promoting operational synergies and management optimization.

Especially:

1. The following staff functions provided by the Parent Company operate in support of the Group companies:

- Internal Audit;
- General Counsel & Sustainability (Corporate, Insurance and Compliance, Litigation and Contracts, Export Control and Claims & Contract Management, Sustainability);
- Quality Assurance;
- CPO (People & Culture & IT);
- CFO (Finance: Controlling Romania & minors, Consolidation, Controlling, Treasury & networking Capital).

2. The following functions have been centralized:

- Commercial (Sales, Wte & Special Projects, Proposal, Mkt & Communication);
- Operation (Engineering, Construction & Commissioning, Quality & Welding, Supply Chain, Project Management, SWS);
- Service (Service Sales & proposal, Service Operation, Service Spare Parts & Spir).

6.4 Supervisory Body (SB)

The Company has defined that the SB will be composed of a minimum of three and a maximum of five members who will be appointed by the Board of Directors; following the formal acceptance of the appointed subjects, communication is given by means of a special service order. A conviction (or plea bargain) will be a cause of ineligibility as a member of the SB, even if not irrevocable, for having committed one of the crimes referred to in Legislative Decree 231/2001 or the conviction (or plea bargaining) to a penalty that involves the interdiction, even temporary, from public offices or the temporary interdiction from the management offices of legal persons or companies.

The members of the SB appointed by the Company on the basis of Article 6 of Legislative Decree 231/01 and the Confindustria Guidelines must be identified on the basis of the following requirements:

Integrity and morality

The members of the SB must submit declarations of integrity in accordance with current regulations.

Autonomy and Independence

The SB must be autonomous and independent and must not be directly involved in the management activities that are the subject of its control activity, as the objectivity of judgment in the conduct checks and the effectiveness of the Model would be questioned.

Professionality

The SB must have adequate technical and professional skills to be able to effectively carry out the assigned activity. These are specialized techniques specific to those who carry out this activity, such as the ability to analyse and assess corporate risks and their containment measures, the identification of points of weaknesses in processes and related procedures, as well as methodologies for detecting fraud, etc.

These techniques must be applied both as a preventive measure in order to adopt the most appropriate measures to prevent the commission of the offences with reasonable certainty, and in hindsight to ascertain whether the offence has been committed. As part of the role held by the members of the SB, the company asks for **continuity of action** with regard to the constant supervision of the effectiveness of the Organisational Model, its continuous implementation and updating. The SB must also provide advisory opinions on the construction of the Organisational Model so that any weaknesses are highlighted; the advisory opinion does not affect the independence and objectivity of judgement in specific events.

The SB may make use of the Internal Audit Function to carry out the verification and control activities envisaged by the Organisational Model, as well as the corporate functions that may be useful from time to time in carrying out activities that require specific professional content. The tasks that the SB will have to carry out are:

a) verify the application of the Organizational Model in relation to the different types of crime;
b) evaluate and monitor the effectiveness of the Organizational Model in relation to its ability to prevent the commission of crimes;
c) propose to the Managing Director and the Board of Directors, where necessary, the updating and amendments to the Organisational Model itself in relation to the changed regulations and company conditions;
d) monitor initiatives for the dissemination of knowledge and understanding of the Model.

On an operational level, the SB's activity consists of:

- define an intervention plan of periodic checks aimed at activities at risk as defined in the Organizational Model;
- collect and store relevant information in compliance with the Organisational Model as well as update the list of information that must be sent to the SB;
- conduct the internal investigations necessary to ascertain alleged violations brought to the attention of the SB by reports or emerged during verification activities;
- periodically check the map of areas at risk of crime in order to adapt it to changes in the company's activities and organization;
- report periodically, at least annually, to the Managing Director and the Board of Statutory Auditors on the implementation of the company policies for the implementation of the Organisational Model.

For the purpose of risk mapping (Crime Matrix 231), management must report to the SB any situations that expose the Company to the risk of crime. In order to be able to carry out the tasks described above, the SB:

- has access to company documents in order to be able to carry out the necessary checks, without prior authorisation from the competent reference offices;
- can make use of the appropriate professional resources and the necessary financial resources;
- can make use of the support of the various company structures that may be involved in the control activity.

The SB has its own Operating Regulations, approving their contents and presenting them to the Board of Directors at the first available meeting following the appointment.

6.4.1 Reporting by the Supervisory Body

The Supervisory Body's reporting is carried out to the Corporate Bodies through two lines:

- the first, on an ongoing basis, directly with the Managing Director;
- the second, on an annual basis, to the Board of Directors and the Board of Statutory Auditors. Every year, the SB sends the Board of Directors a written report on the implementation of the Organisational Model in the Company, requesting the allocation of an adequate budget to carry out supervisory activities, to be managed in full autonomy.

The SB may be convened at any time by the Corporate Bodies or may in turn submit a request to this effect to report on specific situations in the operation of the Organisational Model whenever it deems it necessary or appropriate.

6.4.2 Information flows to the Supervisory Body

Each corporate function is required to inform the Supervisory Body of any fact or change in the processes and tasks that are affected by the Organisational Model applied in the Company pursuant to Legislative Decree 231/01. In this regard, the following must be reported when the event occurs:

- conduct not in line with the rules of conduct adopted by the Company;
- the commission of one of the offences provided for by Legislative Decree 231/2001 or the violation or fraudulent circumvention of the principles and requirements of the Organisational Model;
- changes to the system of proxies and/or changes to the proxies assigned;
- promptly the measures and/or news coming from judicial police bodies or any other authority;
- requests for legal assistance forwarded by corporate bodies for the crimes referred to in the Decree;

- the reports prepared by the heads of the company functions that contain facts, acts, events and omissions relating to the crimes referred to in the Decree;
- the implementation of the disciplinary measures and sanctions proposed by the SB.

Whistle-blowers, whose identity is not disclosed, are protected against all forms of discrimination, penalization and retaliation for reasons related to the report. The SB, in fact, guarantees the absolute confidentiality and anonymity of the reporting persons, without prejudice to legal obligations and the protection of the Company's rights.

Reports received by the SB must be collected and stored in a special archive to which access is allowed only by members of the SB.

Although the SB, in accordance with the Code of Ethics, considers reports not transmitted anonymously to be preferable, anonymous reports are also allowed. In this case, the SB shall first assess their validity and relevance with respect to its tasks; anonymous reports that contain facts relevant to the tasks of the SB and not facts of generic, confusing and/or patently defamatory content.

Reports must be communicated to the Supervisory Body either by direct communication or, for employees, through the Heads of Departments, who must promptly transmit the original of what has been received to the Supervisory Body, using confidentiality criteria to protect the effectiveness of the investigations and the integrity of the persons involved in the report.

The members of the Supervisory Body, as subjects authorized to process data pursuant to privacy legislation, require that the data contained in the reports forwarded are relevant to the purposes referred to in Legislative Decree 231/2001.

In the detailed description of the conduct that gives rise to the report, information not strictly related to the subject of the report must not be provided. In the event of reports produced in obvious bad faith, the SB reserves the right to archive them by deleting the names and elements that may allow the identification of the reported subjects.

The Company, in accordance with the provisions of Law 179/2017, containing the "*Provisions for the protection of whistle-blowers of crimes or irregularities of which they have become aware in the context of a public or private employment relationship*", protects whistle-blowers from acts of retaliation or discrimination, direct or indirect, for reasons connected, directly or indirectly, to reporting.

All communications by the reporting party to the Supervisory Body may be made, alternatively and without preference, by:

- E-mail;
- Note/letter.

For contact with the SB, the Company has set up the following e-mail address reserved for the SB itself to which reports can be sent: odv@acboilers.com; alternatively, the reports may happen using the company platform, by accessing the link: sofinter.integrityline.com.

The postal address is: Supervisory Body at General Counsel & Sustainability – Piazza Buffoni, 3 – 21013 Gallarate (VA).

6.4.3 Whistleblowing

On 29 December 2017, Law no. 179 of 30 November 2017 came into force, containing the "Provisions for the protection of whistle-blowers of crimes or irregularities of which they have become aware in the context of a public or private employment relationship", which intervened on art. 54-bis of Legislative Decree no. 165/2001 and art. 6 of Legislative Decree 231/2001.

On the other hand, with regard to the innovations introduced by Law no. 179/2017 (Provisions for the protection of whistle-blowers of crimes or irregularities of which they have become aware in the context of a public or private employment relationship) on the subject of "Whistleblowing", the organisational model must now provide:

1) one or more channels that allow those who in any capacity represent or manage the entity to submit, in order to protect the integrity of the entity, detailed reports of illegal, relevant and factual conduct or violations of the organisational and management model of the entity, of which they have become aware due to the functions performed, these channels guarantee confidentiality of the identity of the whistle-blower in the management of the report;

2) at least one alternative reporting channel suitable for ensuring, by electronic means, the confidentiality of the reporting identity;

3) appropriate measures to protect the identity of the whistle-blower and to maintain the confidentiality of the information in any context subsequent to the report, to the extent that anonymity and confidentiality are enforceable by law.

The law on whistleblowing introduces into the Italian legal system a set of rules aimed at improving the effectiveness of the tools to fight corruption, as well as protecting the whistle-blowers more intensely, encouraging the use of the tool of reporting illegal conduct or violations of organisational, management and control models.

Given that the Company, in the absence of a specific regulatory provision, until the introduction of the Whistleblowing Law, has always paid particular attention to the issue of reporting, also regulating the flows of information, as provided for in paragraph 6.4.2.

In order to implement the additions made to art. 6 of Legislative Decree 231/2001, it was necessary to integrate the Model with a system for managing reports of wrongdoing that makes it possible to protect the identity of the whistle-blower and the related right to confidentiality also through the introduction within the disciplinary system of specific sanctions imposed in the event of any acts of retaliation and discriminatory attitudes to the detriment of the whistle-blower who, in good faith and on the basis of reasonable factual elements, has reported unlawful conduct and/or in violation of the Model and the Code of Ethics.

That said, the Company, in order to ensure the effectiveness of the whistleblowing system, has adopted the Whistleblowing Procedure which informs employees of the existence of special communication channels that allow them to submit any reports, based on precise and agreed factual elements, also guaranteeing the confidentiality of the identity of the whistle-blower by electronic means.

7. USE OF ARTIFICIAL INTELLIGENCE SYSTEMS

The Company permits the use of Artificial Intelligence systems exclusively for lawful business purposes and in compliance with applicable laws, the Code of Ethics, internal procedures, and provisions regarding the protection of personal data, information security, and intellectual property. It is prohibited to use Artificial Intelligence tools unauthorized by the Company or to include confidential data, information, personal data, or content subject to confidentiality restrictions without the necessary authorizations and guarantees.
The output generated by Artificial Intelligence systems must be subject to prior verification and validation by the personnel responsible, who retain full responsibility for the decisions made and the documents produced.
The Company adopts adequate organizational and control measures to prevent the risk of committing crimes set forth in Legislative Decree 231/2001 related to the use of Artificial Intelligence systems.
Sofinter Group has adopted the Corporate Policy for the Responsible Use of Artificial Intelligence and has established and appointed the Artificial Intelligence Committee ("AI Committee"). The AI Committee acts as the governance body in charge of ensuring structured, responsible, and compliant management of the AI systems used within the Group, in accordance with applicable laws and company policies.
The Supervisory Board receives periodic information flows regarding the use of these tools and any anomalies or violations detected.
Violation of the provisions relating to the use of Artificial Intelligence constitutes non-compliance with Model 231 and is subject to the disciplinary measures provided for by the company's sanctions system.

8. SUSTAINABILITY GOVERNANCE AND ESG RISK MANAGEMENT

The Company integrates ESG factors into decision-making processes, internal controls, and risk management, in alignment with the Code of Ethics and the Supplier Code of Conduct. Monitoring covers relevant ESG indicators, including Scope 1, 2, and 3 emissions, energy, water, waste, health and safety, people, ethics, and sustainable procurement.

8.1 Sustainable supply chain and CBAM

Supplier selection and monitoring incorporate ethical, social, and environmental criteria, as well as the traceability and reliability of ESG data, prioritizing strategic, critical, or high-risk suppliers. Acceptance of the Supplier Code of Conduct is a prerequisite for the business relationship:

- extension of the Code's principles to relevant sub-suppliers;
- suspension or termination of the relationship in the event of serious violations, unreliable data, or lack of cooperation.

The Company ensures compliance with applicable CBAM requirements, including authorization, declarations, certificates, and emissions verification.
Violations of the Code, falsification or concealment of data, and significant non-compliance issues are reported to the Supervisory Body in accordance with established reporting procedures.

9. DISCIPLINARY SYSTEM

9.1 General principles

It is essential for the effectiveness of the Organizational Model to build an adequate sanctioning system for the violation of the rules of conduct contained in the Code of Ethics and the failure to comply with the measures indicated in the model itself. The sanctions provided for will be applied to any violation of the rules of corporate conduct and the provisions contained in the Model, including the implementation of actions or conduct that do not comply with the provisions of the Whistleblowing Law pursuant to Law 179/2017 and any subsequent amendments and additions, regardless of the possible outcome of the criminal trial, as these rules are assumed by the Company in full autonomy and also disregard the conduct that may result in crimes.

9.2 Penalties against employees

Violations of the rules of conduct contained in the Company's Code of Ethics are considered disciplinary offences. The sanctions payable to employees are among those provided for by the Company Regulations, in compliance with the procedures provided for by art. 7 of the Workers' Statute (Law no. 300 of 20 May 1970) and any applicable social regulations. This Organisational Model refers to the categories of sanctionable facts provided for in the National Labour Contract applied in the company; these categories describe the sanctioned behaviours based on the importance of the individual cases considered and the sanctions actually envisaged for the commission of the facts depending on the seriousness. In particular, with reference to Article 8 title seven of the National Labour Contract for employees in the private metalworking industry and plant installation, failure by employees to comply with the provisions and procedures contained in this Organisational Model will result in the application of the following sanctions in proportion to the seriousness of the infringement:

1. VERBAL WARNING OR WRITTEN WARNING;
2. FINE;
3. SUSPENSION FROM SERVICE AND REMUNERATION;
4. DISMISSAL WITH NOTICE;
5. DISMISSAL WITHOUT NOTICE.

Any violation of the rules provided for by the Model or referred to therein and, in any case, the commission (even in the form of an attempt) of any criminal offence for which Legislative Decree 231/01 is applicable constitutes a disciplinary offence. Failure to comply with the confidentiality obligations on the identity of the whistle-blower provided for by the Law on whistleblowing pursuant to Law 179/2017 and any subsequent amendments to protect the employee or collaborator who reports wrongdoing, the performance of acts of retaliation or discrimination against the person reporting the report, as well as the conduct of the person who makes a report with intent or gross negligence that proves to be unfounded also constitutes a violation of the Model. The powers already conferred on company management, within the limits of their respective competences, remain unchanged both for the verification of infringements and for disciplinary measures. The disciplinary system is subject to validity and application checks by the functions in charge together with the Management and the Head of Human Resources management.

9.3 Measures against Managers

In the event of violation by the Managers of the internal procedures provided for by the Organisational Model in the performance of sensitive activities, or conduct that does not comply with the requirements of the Organisational Model itself and the Code of Ethics, as well as the Whistleblowing Law and the application procedure, the Company will apply, with regard to those responsible, the most appropriate measures in accordance with the provisions of Article 7 of the Workers' Statute (Law no. 300 of 20 May 1970) and the National Collective Labour Agreement for Executives applied, as such violations will be considered by the Company as non-compliance with the obligations arising from the employment relationship.

9.4 Measures against Directors and Statutory Auditors

Violations of the Organisational Model, the Code of Ethics and the current legislation on whistleblowing and the application procedure by the Directors and Statutory Auditors are reported by the Supervisory Body to all members of the Board of Directors and the Board of Statutory Auditors who will take appropriate measures and initiatives in accordance with the law, to convene the Shareholders' Meeting, where necessary, in order to adopt the most suitable measures provided for by law.

9.5 Measures against Consultants and Partners

The violation by Consultants or Partners of the rules of conduct referred to in the Organizational Model and the Code of Ethics or the commission of the crimes provided for by Legislative Decree 231/2001, is sanctioned according to the provisions of the contractual clauses included in the relevant contracts and, in the event of serious non-compliance, also with the termination of the contractual relationship. This is without prejudice to any claim for compensation in the event that the conduct results in concrete damage to the Company.

9.6 Measures applicable to the recipients of reports ("Whistleblowing")

In the event of violation of the regulatory provisions on whistleblowing and the application procedure in order to protect the identity of the whistle-blower and the same from any acts of retaliation or discrimination, the Company may apply the following sanctions against the SB. In the event that one of the members of the SB violates the confidentiality of the identity of the whistle-blower, the other members will immediately notify the Board of Directors so that it can proceed with the revocation of the office of the defaulting member and the consequent appointment of his or her replacement. If, on the other hand, the violation of the confidentiality of the identity of the whistle-blower by the SB as a whole is ascertained, the Board of Directors will proceed with the revocation of the appointment and the consequent appointment of the entire Body in addition to any further provisions of law.

10. MAPPING OF POTENTIAL RISKS OF PREDICATE OFFENCES

Pursuant to the provisions of Article 6, paragraph 2, letter a) of the Decree, the Company, through a risk mapping process, has identified the Areas of activity in which crimes may potentially be committed among those provided for by the Decree. It should also be noted that some functions – areas of activity, although not directly giving rise to a risk of crime, may be the "implementing arm" of the hypothesis of crime committed by another Area. The latter, despite being identified as a potential risk area, can "contaminate" and make other areas "complicit" without them realizing that they are participating in an offence or crime.
Also for these areas of intervention, the Procedures of the Organizational Model provide for checks on the management and organization of the process in its entirety. Specifically, these are the following areas:

1. methods of managing financial resources (e.g. management systems of financial resources, both incoming and outgoing, which may involve atypical financial flows);
2. management of inspections (e.g. Legislative Decree 81/2008, tax audits, INPS, etc. and any disputes that arise from it);
3. management of ordinary obligations (e.g. administrative practices, management of possible judicial and extrajudicial disputes with the P.A.);
4. management of the purchase order issuing process (procurement process of goods and services with reference to purchases managed by the competent units of the Company and/or managed by means of a service contract, the phases of the process relating to the procurement request, the selection of the supplier and the stipulation of the contract, the use and management of contracts, the review of contracts stipulated);
5. utility management process with particular reference to the management of gifts, sponsorships, donations and entertainment expenses;
6. process of procurement, purchase and sale of raw materials and products on the market with particular reference to the phases of selection of the counterparty, negotiation and stipulation of the contract;
7. human resources selection and recruitment process;
8. management of the process of approving invoices for payment;
9. companies or entities belonging to the same group but based in different countries for the following transactions: (i) Intra-group purchase and/or sale contracts; (ii) Management of cash flows; (iii) Intragroup investments.

The result of the analysis of the processes and functions, carried out by the Company, is the Crime Matrix 231, which highlights the sensitive activities of offences and the responsibilities of the functions involved. The Company has adopted specific Control Protocols and procedures aimed at avoiding the commission of the crimes provided for by Legislative Decree 231/2001, considered potential on the basis of the analysis carried out of sensitive processes. The Crime Matrix is an integral part of the Organizational Model and represents the tool that identifies the areas and intensity of the risk of committing the crimes provided for by the law. It also represents the main tool for the implementation, verification and continuous improvement of the Organisational Model consistent with Legislative Decree and constitutes a useful information basis for the SB from which to start observation and investigation aimed at continuous improvement.
The documentation relating to the Crimes-Sensitive Activities matrix and the risk measurement and control model is filed with the Company's Legal and Corporate Compliance Department.

11. UPDATE OF THE ORGANIZATIONAL MODEL

Since this Organisational Model is an "act of enactment of the Management Body" (in accordance with the provisions of Article 6, paragraph 1, letter a of the Decree), its adoption, as well as subsequent amendments and additions, also on the proposal of the Supervisory Body, are subject to the competence of the Company's Board of Directors.
The Director with appropriate powers is also granted the right to make any formal and non-substantial amendments or additions to the text, periodically reporting to the Company's Board of Directors on the aforementioned changes.
In the context of these powers, the Director may also adopt or modify the company procedures and control protocols relating to the sensitive company areas indicated in this Model and in the 231 Crimes Matrix.
In any case, the Organisational Model, the procedures and control protocols relating to the sensitive processes indicated therein must be promptly amended:

- if there are significant changes in the regulatory system;
- if there are significant changes in the corporate and/or organizational structure of the company;
- when violations or circumvention of the requirements are identified, in order to maintain the efficiency of the Organizational Model.

The Supervisory Body has the task of monitoring the progress and results of the update of the Organisational Model and any changes to the control procedures and protocols, providing adequate information to the Company.

12. REFERENCE DOCUMENTS FOR THE PREPARATION OF THE ORGANISATIONAL MODEL

A. Group Code of Ethics
B. Supplier Code of Conduct
C. Quality System: quality manual and procedures
D. Occupational Safety Management System
E. Legislative Decree 231/01
F. Confindustria Guidelines

13. ANNEXES TO THE ORGANISATIONAL MODEL

Organizational Model – Special Part
Crime Matrix 231 – Sensitive business activities
Control Protocols
Anti-Corruption Manual

Appendix: Evolution of the Organizational Model

DATE	*DESCRIPTION*
October 28, 2004	**Organizational Model / ISSUE 1**
October 28, 2004	**Code of Ethics / ISSUE 1**
March 24, 2006	**Organizational Model / ISSUE 2** Approval of the Organizational Model – Issue 2, which incorporated: - the new regulations on Legislative Decree 231/01; - the organisational changes that have taken place since 28 October 2004.
March 29, 2007	**Organizational Model / ISSUE 3** Approval of the Organizational Model – Issue 3, which has: - the minimum number of members of the SB has been reduced, from three to two; - updated the Company's shareholdings and consequently Annex 1.
October 30, 2008	**Organizational Model / ISSUE 4** Approval of the Organizational Model – Issue 4, which has: - updated the Company's shareholdings and consequently Annex 1; - implemented the regulations relating to: (i) IT crimes and unlawful processing of data introduced by Law no. 48 of 18 March 2008, art. 7; (ii) manslaughter and serious or very serious culpable injuries, committed in violation of accident prevention regulations and on the protection of hygiene and health at work (pursuant to Article 25-septies of Legislative Decree 231/01) introduced by Law No. 123 of 3 August 2007, Article 9; (iii) offences of receiving stolen goods, money laundering and use of illicit utilities (pursuant to Article 25-octies of Legislative Decree 231/01 introduced by Legislative Decree No. 231 of 21 November 2007, Article 63); (iv) acknowledged changes in the company organization.
July 8, 2011	**Organizational Model / ISSUE 5** It implements the regulations relating to: • Offences relating to copyright infringement and inducement not to make declarations or to make false declarations to the judicial authorities (pursuant to Article 25-novies and Article 25-decies of Legislative Decree 231/01), • Article 10 of Law No. 146 of 16 March 2006 – "Ratification and Implementation of the United Nations Convention and Protocols against Transnational Organized Crime, adopted by the General Assembly on 15 November 2000 and 31 May 2001" published in the Official Gazette No. 85 of 11 April 2006 – Ordinary Supplement No. 91.
March 27, 2013	**Code of Ethics / ISSUE 2**
March 28, 2014	**Organizational Model / ISSUE 6** It implements the regulations relating to: ***Art. 25-undecies***: *"Environmental Crimes"* ***Art. 25-duodecies***: *"Employment of workers without a residence permit"*
March 24, 2017	**Organizational Model / ISSUE 7, which has implemented:** - new regulations regarding Legislative Decree 231/01 (Self-laundering and Law 9/2013); - changes to the company organization; - adoption and approval of the Operating Regulations by the Supervisory Body; - introduction of the update of the Organizational Model; - introduction of the new attachments – Crime Matrix and Anti-Corruption Manual.
December 1, 2017	**Code of Ethics / ISSUE 3**
January 26, 2018	**Organizational Model / ISSUE 8, which has implemented:** - changes in the company organization; - among the tasks of the Supervisory Body, the possibility of accessing company documents in order to carry out the necessary checks, without prior authorization from the competent reference offices; - annual request of the Supervisory Body to the Board of Directors for the allocation of an

	adequate budget for carrying out supervisory activities, to be managed in full autonomy.
May 25, 2018	**Organizational Model / ISSUE 9, which has implemented:** - changes in the company organization; - new regulations regarding Legislative Decree 231/01 (Art. 25-terdecies Racism and xenophobia); - Reporting of the SB on a six-monthly basis to the BoD and the Board of Statutory Auditors; - Changes in information flows to the SB and in reports to the SB.
February 21, 2019	**Code of Ethics / ISSUE 4**

October 22, 2021	**Organizational Model / ISSUE 10**
	It transposes:
	- the new regulations on Legislative Decree 231/01:
	  - Article 25-ter letter s-bis: "Corruption between private individuals" (Article 2635 of the Italian Civil Code) and "Incitement to corruption between private individuals" (Article 2635 bis of the Italian Civil Code);
	  - Article 25-quaterdecies: "Fraud in sports competitions, abusive exercise of gaming or betting and games of chance exercised by means of prohibited machines" [article added by Law no. 39/2019];
	  - Art. 25-quinquiesdecies: "Tax crimes" [article added by Law no. 157/2019 and by Legislative Decree no. 75/2020];
	  - Art. 25-sexiesdecies: "Smuggling" [article added by Legislative Decree no. 75/2020];
	  - New types of tax crimes including the crimes of: unfaithful declaration, failure to declare, undue compensation, fraudulent declaration through the use of false invoices and smuggling, and the implementation of the so-called PIF Directive no. 1371/2017 of the European Parliament and of the European Council of 5 July 2017, laying down rules for the "*fight against fraud affecting the financial interests of the Union by means of criminal law";*
	- changes in the company organization;
	- par. 6.4.3 Whistleblowing: the protection by the Company, in accordance with the provisions of Law 179/2017, of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship;
	- par. 7.6 Measures applicable to the recipients of reports ("Whistleblowing").

April 2022	**Organizational Model / ISSUE 10** It implements the new regulations on Legislative Decree 231/01: - Article 25 octies 1 "Offences relating to means of payment other than cash"; - Art. 25-septiesdecies: "Crimes against cultural heritage" [Law no. 22 of 9 March 2022]; - Art. 25-duodevicies: "Laundering of cultural property and devastation and looting of cultural and landscape property".
December 12, 2024	**Organizational Model / ISSUE 11** It transposes: - the new regulations on Legislative Decree 231/01; - changes in the company organization and corporate structure; - the reference to the Whistleblowing Procedure and the new reporting channel; - the reference to the New Supplier Code of Conduct.
February 26, 2026	**Organizational Model / ISSUE 12** It transposes: - new regulations on Legislative Decree 231/01; - changes in the company organization and corporate structure.
May 26, 2026	**Organizational Model / ISSUE 13** It transposes the reform of environmental crimes – Legislative Decree 21 April 2026 – Special Part.

October 23, 2026	**Organizational Model / ISSUE 14** It transposes: - the new regulation under Legislative Decree 231/01 (Art. 25-vicies: "Offenses committed using artificial intelligence"); - reference to the use of Artificial Intelligence systems; - reference to sustainability governance and the oversight of ESG risks; sustainable supply chain and CBAM.

This **Organizational Model – Issue no. 14** was approved by the Managing Director the Company, by virtue of the authority delegated to him by the Board of Directors, on October 23, 2026 and replaces previous editions.

ORGANIZATIONAL MODEL – SPECIAL PART

The purpose of the Special Section is to define guidelines, rules and principles of conduct that all recipients of Model 231 must follow in order to prevent, in the context of the specific sensitive activities carried out in the company, the commission of offences provided for by the Decree and to ensure conditions of fairness and transparency in the conduct of corporate activities.
In general, all company representatives must adopt, each for the aspects of their competence, conduct in accordance with the contents of the following documents:

- Model 231
- Code of Ethics
- Procedures and provisions
- Powers of attorney and proxies
- Service orders
- Organizational communications
- Safety and environmental management systems
- Any other document that regulates activities falling within the scope of application of the Decree

It is also expressly forbidden to adopt conduct contrary to the provisions of the law in force.

THE CONTROLS OF THE SUPERVISORY BODY

Without prejudice to the provisions of the General Part relating to its powers and duties, including the discretionary power to carry out specific checks following the reports received, the Supervisory Body periodically carries out checks on potentially risky activities, aimed at verifying the correct implementation of the same in relation to the rules set out in this Model, committed in the interest or to the advantage of the company.
The Supervisory Body must examine reports of alleged violations of the Model and carry out the investigations deemed necessary or appropriate.
To this end, the Supervisory Body is guaranteed free access to all relevant company documentation.

LIST OF CRIMES PROVIDED FOR BY LEGISLATIVE DECREE 231/01

List of criminal offences provided by Legislative Decree 231/01:
Undue receipt of grants, fraud against the State, a public body or the European Union or for the purpose of obtaining public grants, computer fraud against the State or a public body and fraud in public supplies - Art. 24 [Article amended by Law 161/2017 and Legislative Decree no. 75 of 14 July 2020]
IT crimes and unlawful data processing - Art. 24 bis [Article added by Law 48/2008, amended by Legislative Decrees no. 7 and no. 8/2016, by Legislative Decree no. 105/2019 and by Law n. 90 of 28 June 2024]
Organized crime crimes - Art. 24 ter [Article added by Law no. 94/2009, amended by Law 69/2015]
Embezzlement, extortion, undue inducement to give or promise benefits, corruption, misappropriation of money or movable property - Art. 25 [Article amended by Law no. 190/2012 and Law no. 3 of 9 January 2019 and by Legislative Decree no. 75 of 14 July 2020. Title amended, together with the text, by conversion law n. 112 of 8 August 2024]
Counterfeiting of coins, public credit cards, stamped securities and instruments or signs of recognition - Art. 25 bis [Article added by Legislative Decree no. 350/2001, converted with amendments by Law no. 409/2001; amended by Law no. 99/2009; amended by Legislative Decree no. 125/2016]
Crimes against industry and commerce - Art. 25 bis 1 [Article added by Law no. 99/2009]
Corporate Crimes - Art. 25 ter [Article added by Legislative Decree no. 61/2002, amended by Law no. 190/2012, by Law 69/2015 and subsequently by Legislative Decree no. 38/2017 and by Legislative Decree no. 19 of 2 March 2023]
Crimes for the purpose of terrorism or subversion of the democratic order provided for by the Criminal Code and special laws - Art. 25 quater [Article added by Law no. 7/2003]
Female genital mutilation practices - Art. 25 quater 1 [Article added by L. n. 7/2006]
Crimes against the individual personality - Art. 25 quinquies [Article added by Law no. 228/2003 and amended by Law no. 199/2016]
Market abuse crimes - Art. 25 sexies [Article added by Law no. 62/2005] and other market abuse offences [Article amended by Legislative Decree no. 107/2018 and Law no. 238 of 23 December 2021]
Manslaughter or serious or very serious injury committed in violation of the rules on health and safety at work Art. 25 septies [Article added by Law no. 123/2007]
Receiving stolen goods, laundering and use of money, goods or utilities of illegal origin, as well as self-laundering – Art. 25-octies [Article added by Legislative Decree 231/2007; amended by Law no. 186/2014 and Legislative Decree no. 195 of 18 November 2021]
Crimes relating to non-cash payment instruments and fraudulent transfer of assets – Article 25 octies-1 [Article added by Legislative Decree No. 184 of 18 November 2021 and amended by Legislative Decree No. 105 of 10 August 2023 coordinated with Conversion Law No. 137 of 9 October 2023]
Crimes relating to violations of European Union restrictive measures - Art. 25 octies-2 [Article added by Legislative Decree no. 211 of 30 December 2025]
Crimes relating to violation of copyright – Art. 25 novies [Article added by Law no. 99/2009]
Inducement not to make declarations or to make false declarations to the judicial authority – Art. 25 decies [Article added by Law no. 116/2009]
Environmental crimes – Art. 25 undecies [Article added by Legislative Decree 121/2011, amended by Law no. 68/2015, by Legislative Decree no. 21/2018, by Legislative Decree n. 116 of 8 August 2025 , by Law n. 147 of 3 October 2025 and by Legislative Decree n. 81 of 21 April 2026]
Employment of illegally staying third-country nationals – Article 25k [Article added by Legislative Decree No. 109/2012 and amended by Law No. 161/2017]
Racism and xenophobia – Art. 25 terdecies [Article added by Law no. 167/2017 and amended by Legislative Decree no. 21/2018]
Fraud in sports competitions, unauthorized gambling or betting and gambling carried out by means of prohibited devices – Art. 25-quaterdecies [Article added by art. 5 of Law no. 39/2019]
Tax crimes – Art. 25 quinquiesdecies [Article added by Legislative Decree no. 124/2019 coordinated with Conversion Law no. 157/2019 and amended by Legislative Decree no. 75/2020 and by Legislative Decree no. 156/2022]
Smuggling – Art. 25 sexiesdecies [Article added by Legislative Decree no. 75/2020 and amended in the text by Legislative Decree n. 141 of 26 September 2024]
Provisions on crimes against cultural heritage – Art. 25 septiesdecies [Article added by L.n. 22 of 09 March 2022]
Recycling of cultural assets and devastation and plundering of cultural and landscape assets – Art. 25 duodevicies [Article added by L.n. 22 of 09 March 2022]
Provisions regarding crimes against animals - [Art. 25 undevicies Article added by Law n. 82 of 6 June 2025]
Offences Committed Through Artificial Intelligence Systems - [Art. 25-vicies added by Legislative Decree No. 160 del 2026]
Attempted Crimes – Art. 26
Liability of entities for administrative offences deriving from a crime [They constitute a prerequisite for entities operating in the virgin olive oil supply chain] - Art.12 L. 9/2013
Transnational crimes [The following crimes constitute a prerequisite for the administrative liability of entities if committed in a transnational manner] - L. 146/2006.

Crimes pursuant to Article 24-*bis* of Legislative Decree 231/2001
Computer crimes and unlawful data processing

Regulatory references:
- Abusive access to an IT and telematic system (Article 615-*ter*, Criminal Code);
- Illegal possession, distribution and installation of equipment, codes and other means capable of accessing computer or telematic systems (Article 615-*quater*, Criminal Code);
- Illegal possession, distribution and installation of computer equipment, devices or programs aimed at damaging or interrupting a computer or telematic system (art. 615-*quinquies*, Criminal Code) – REPEALED BY LAW NO. 90 OF 28 JUNE 2024;
- Illegal possession, distribution, and installation of equipment and other means for intercepting, preventing, or interrupting telegraphic or telephone communications or conversations (Article 617-*bis* of the Criminal Code);
- Illegal interception, impediment, or interruption of computer or electronic communications (Article 617-*quater* of the Criminal Code);
- Illegal possession, distribution, and installation of equipment and other means for intercepting, preventing, or interrupting computer or electronic communications (Article 617-*quinquies* of the Criminal Code);
- Falsification, alteration, or suppression of the content of computer or electronic communications (Article 617-*sexies* of the Criminal Code);
- Mitigating circumstances (Article 623-*quater* of the Criminal Code);
- Extortion (Article 629 of the Criminal Code);
- Damage to information, data, and computer programs (Article 635-*bis* of the Criminal Code);
- Damage to public or public-interest information, data, and computer programs (Article 635-*ter* of the Criminal Code);
- Damage to computer and telematic systems (Article 635-*quater* of the Criminal Code);
- Illegal possession, distribution, and installation of computer equipment, devices, or programs intended to damage or disrupt a computer or telematics system (Article 635-*quater*.1, Criminal Code);
- Damage to computer and telematic systems of public utility (Article 635-*quinquies* of the Criminal Code);
- Mitigating circumstances (Article 639-*ter* of the Criminal Code);
- Computer documents (Article 491-*bis* of the Criminal Code);
- Computer fraud (Article 640-*ter*);
- Computer fraud by a person providing electronic signature certification services (Article 640-*quinquies* of the Criminal Code);
- Violation of the provisions regarding the National Cybersecurity Perimeter (Article 1, paragraph 11, Legislative Decree No. 105 of October 21, 2019).

Sensitive activities
Article 6, paragraph 2, letter a) of the Decree indicates, as one of the essential elements of the organisational, management and control models provided for by the Decree, the identification of the so-called "sensitive" activities, i.e. those activities of the company in the context of which there could be a risk of committing one of the offences expressly referred to in the Decree.
The analysis of the company's processes has made it possible to identify the following "sensitive" activities, in the context of which the types of crime referred to in Art. 24-*bis* of Legislative Decree no. 231/2001 could theoretically occur:
- ✓ abusive access to systems and/or disclosure, interception or theft of information of an info-telematic nature (including access credentials) and/or use of computer programs in order to acquire or illegally disseminate information of a confidential nature, or to destroy, damage or render useless third-party computer systems. The risk profile can also be achieved through activities carried out by third parties;
- ✓ alteration or falsification of deeds, documents and records prepared and sent electronically.

The potential associated crimes are:
- ✓ abusive access to a computer or telematic system;
- ✓ possession and abusive dissemination of access codes to computer or telematic systems;
- ✓ dissemination of equipment, devices or computer programs aimed at damaging or interrupting a computer or telematic system;
- ✓ unlawful interception, impediment or interruption of computer or telematic communications;
- ✓ installation of equipment to intercept, prevent or interrupt computer or telematic communications;
- ✓ damage to information, data and information programs used by the State or by another public body or in any case of public utility;
- ✓ falsehoods relating to electronic documents.

Organizational system control tools
This Special Section provides for the express obligation, by the company representatives directly and, through specific contractual clauses, on external collaborators and partners, to avoid all conduct that constitutes the crimes described above. The system for the prevention of crimes perfected by the company has been created by applying the following control standards to sensitive activities:
- the existence of a policy on the security of the information system;
- the adoption and implementation of a regulatory instrument that defines the roles and responsibilities in managing the methods of access of internal users to the company and their obligations in the use of IT systems;

- the adoption and implementation of a regulatory instrument that provides for controls in order to prevent unauthorized access, damage and interference to the premises and the goods contained therein through the safety of areas and equipment;
- the adoption and implementation of a regulatory instrument that ensures the correctness and security of the operation of information systems through control policies, procedures and protocols;
- the adoption and implementation of a tool that regulates access to information, information systems, the network, operating systems and applications;
- the adoption and implementation of a tool that defines appropriate modalities for the treatment of incidents and problems related to cybersecurity;
- the adoption and implementation of a regulatory instrument that regulates the roles, responsibilities and operating methods of the activities of periodic verification of the efficiency and effectiveness of the IT security management system;
- the adoption and implementation of a regulatory instrument that defines the roles and responsibilities in the management of purchases of software and IT equipment.

The offences pursuant to Article 24-*ter* of Legislative Decree 231/2001
Organized crime offences

Regulatory references:
- Art. 416 Criminal Code (Criminal association);
- Art. 416-*bis* Criminal Code (Mafia-type association, including foreign associations);
- Art. 416-*bis*.1 Criminal Code (Aggravating and mitigating circumstances for crimes related to mafia activities);
- Art. 416-*ter* Criminal Code (Mafia-political electoral exchange);
- Art. 630 Criminal Code (Kidnapping for the purpose of extortion);
- Art. 74 DPR 309/1990 (Association for the purpose of illicit trafficking of narcotic or psychotropic substances).

Sensitive Areas
In light of the results of the risk assessment carried out by the company, the following areas of business were found to be relevant in relation to the risk of committing organised crime offences:
- ✓ Finance, Treasury & Networking Capital and Controlling
- ✓ Sales/Proposal
- ✓ Integrated Supply Chain
- ✓ Client & Field Service

The following are considered to be risk activities, by way of example, but not limited to:
- ✓ in the context of extraordinary transactions, through the improper management of the role held by the Company in order to promote, finance, establish, organise or participate in associations, both national and transnational, including those aimed at terrorist activities or subversion of the democratic order, and also in the event of cooperation between members of the Company and two or more parties for the prosecution of any non-culpable offence;
- ✓ improper management of the role held within the company in order to promote, establish, organize or participate in associations created through cooperation with two or more subjects for the pursuit of illegal purposes;
- ✓ the crime could be said to be integrated if several subjects referable to the company or together with external parties (suppliers, customers, representatives of the Public Administration, consultants, etc.), associate with the aim of committing several crimes (e.g. against the Public Administration or against industrial property, etc.) also through: a) the financing of the criminal association through the provision of money; b) the hiring of staff or the appointment of consultants or the assignment of jobs to suppliers linked by family ties and/or affinity with members of well-known criminal organizations.

Apart from the hypotheses of participation in the association, the employee of the company could participate in the crime, in the form of external collaboration, in the event that, although not integrated into the organizational structure of the criminal association, he makes a contribution to the achievement of the purposes of the association, for example by facilitating by any means the commission of the crimes for the purpose of the association.

Organizational system control tools
This Special Section, in addition to the specific principles of conduct relating to the areas of risk indicated above, recalls the general principles of conduct provided for in this Model adopted by the company, to which all directors and employees/collaborators of the company are required.
It was considered that, for the prevention of these crimes, the following can perform an adequate preventive function:
- the corporate governance safeguards implemented by the company;
- the control measures provided for by the protocols that are an integral part of the Organisation, Management and Control Model pursuant to Legislative Decree 231/01 adopted by the company;
- the principles set out in the company's Code of Ethics;
- company procedures that are an integral part of the Sofinter Group's Corporate Compliance Program.

Crimes committed in relations with the Public Administration, Corruption and bribery (Articles 24 and 25 and 25-*ter*, limited to the crime of corruption between private individuals of the Decree)

Regulatory references:

- Embezzlement (Art. 314 of the Criminal Code);
- Improper allocation of money or movable property (Art. 314-*bis* of the Criminal Code);
- Embezzlement by profiting from the error of others (Article 316 of the Criminal Code);
- Undue receipt of public funds (Article 316-*ter* of the Criminal Code);
- Embezzlement of public funds (Article 316-*bis* of the Criminal Code);
- Bribery (Article 317 of the Criminal Code);
- Corruption for the exercise of the function (Article 318 of the Criminal Code);
- Corruption for an act contrary to official duties (Art. 319 of the Criminal Code);
- Aggravating circumstances (Article 319-*bis* of the Criminal Code);
- Corruption in judicial acts (Article 319-*ter* of the Criminal Code);
- Undue inducement to give or promise benefits (Art. 319-*quater*);
- Corruption of a person in charge of a public service (Article 320 of the Criminal Code);
- Penalties for the corruptor (Art. 321 of the Criminal Code);
- Incitement to corruption (Article 322 of the Criminal Code);
- Embezzlement, misappropriation of money or movable property, extortion, undue inducement to give or promise benefits, corruption, and incitement to corruption, involving members of international courts or bodies of the European Communities, international parliamentary assemblies, or international organizations, and officials of the European Communities and foreign states (Article 322-*bis* of the Criminal Code);
- Monetary compensation (Article 322-*quater* of the Criminal Code);
- Abuse of office (Article 323 of the Criminal Code); Repealed by Law No. 114 of August 9, 2024;
- Mitigating circumstances (Article 323-*bis* of the Criminal Code);
- Grounds for non-punishability (Article 323-*ter* of the Criminal Code);
- Illicit influence peddling (Article 346-*bis* of the Criminal Code);
- Disruption of the freedom of auctions (Article 353 of the Criminal Code);
- Disruption of the freedom of the contractor selection process (Article 353-*bis* of the Criminal Code);
- Fraud in public procurement (Article 356 of the Criminal Code);
- Fraud (Article 640 of the Criminal Code);
- Aggravated fraud to obtain public funds (Article 640-*bis* of the Criminal Code);
- Computer fraud (Article 640-*ter* of the Criminal Code);
- Applicability of Article 322-*ter* of the Criminal Code (Article 640-*quater* of the Criminal Code);
- Agricultural fraud (Article 2 of Law 898 of December 23, 1986 – Amended by Legislative Decree 184 of November 8, 2021 and Legislative Decree 156 of October 4, 2022);
- Corruption between private individuals (Article 2635 of the Civil Code);
- Incitement to corruption between private individuals (Article 2635-*bis* of the Civil Code);
- Additional penalties (Article 2635-*ter* of the Civil Code).

Definition of Public Administration Entities: "Public Administration Entity" is commonly considered any legal person that takes care of public interests and that carries out legislative, judicial or administrative activities by virtue of public law rules or authoritative acts. Not all natural persons acting in the sphere and in relation to the aforementioned entities are subjects against whom (or by whom) the criminal offences provided for by the Decree are perfected. The figures that take on relevance for this purpose are only those of "**Public Officials**" and "**Public Service Officers**".

Sensitive Areas

For the purposes of the Model, all those business areas which, in order to carry out their typical activities, have relations with the Public Administration (so-called **direct risk**).

Similarly, business areas are to be considered at risk which, although not directly involving the establishment of relations with the Public Administration, manage financial instruments or other types of utilities that could be used to attribute advantages and benefits to public officials (so-called **indirect risk**).

By way of example, and not limited to, the following are for example direct risk activities:

- ✓ participation in all procedures involving relations with the Public Administration;
- ✓ requesting, receiving, using and reporting on public funding, grants and contributions;
- ✓ relations with Public Officials during checks and inspections (Guardia di Finanza, Revenue Agency, Fire Brigade, Inspectors of the ASL, INPS, INAIL, Provincial Police, etc.);
- ✓ stipulation of contracts, conventions and deeds in general with the Public Administration;
- ✓ relations with public entities for the obtaining, maintenance and renewal of authorizations, concessions, licenses, easements, necessary or useful for the exercise of business activities;
- ✓ negotiations, negotiations, private negotiations with public bodies carried out with the Public Administration to obtain orders, contracts, supplies, services, concessions, partnerships, assets, or other similar operations, characterized in any case by the fact that they are carried out in a competitive context, or for the recovery of credits from the PA.

By way of example, and not limited to, the following are considered indirect risk activities:

- ✓ administration, finance and accounting, in which the main risk concerns the hypothesis of setting aside sums of money ("hidden funds") for corrupt purposes;
- ✓ consultancy, which bears the risk that the assignments conceal illicit attributions of utility to subjects linked directly or indirectly to public officials who have direct relations with the company in order to obtain an unfair advantage to the detriment of the Public Administration;
- ✓ management of the procurement of goods and services, which bears the risk that the appointments conceal illicit attributions of utility to persons linked directly or indirectly to public officials who have direct relations with the company, with the sole purpose of altering their independence of judgment and procuring an unfair advantage for the company;
- ✓ judicial and extrajudicial litigation and arbitration proceedings, in which the risk concerns both the hypotheses of corruption in judicial acts and the simulation of transactions to determine the diversion of liquidity from official accounting aimed at feeding hidden funds;
- ✓ gifts, entertainment expenses and sponsorships, which bear the risk that the donations are directly or indirectly addressed to public officials or persons in charge of public service who have direct relations with the company, with the sole purpose of significantly altering their independence of judgment and procuring an unfair advantage for the company.

For details of sensitive activities, conceivable crimes, existing safeguards and risk assessment, please refer to the Matrix Crimes 231 – Sensitive corporate activities – Risks, attached to the Organisational Model.

Organizational system control tools

The Organisation is equipped with organisational tools (organisational charts, organisational communications, procedures, etc.) based on the general principles of:

- clear description of the fill lines;
- knowledgeability, transparency and publicity of the powers attributed (within the entity and towards interested third parties);
- clear and formal delimitation of roles, with a complete description of the tasks of each function, the related powers and responsibilities.

Internal procedures are characterised by the following elements:

- distinction, within each process, between the person who takes the decision (decision-making impulse), the person who executes the decision and the person who is entrusted with the control of the process;
- written record of each relevant step of the process;
- adequate level of formalization.

For the purposes of implementing the rules of conduct in accordance with the provisions of Legislative Decree 231, the Recipients of this Special Part of the Model, in addition to complying with the provisions of the law on the subject, the rules in the Code of Ethics and the principles indicated in the General Part of this Model, must comply with the behavioural protocols, placed to protect the risks of crime identified above and referable to the activities at risk. The system of proxies and powers of attorney contributes, together with the other tools of this Model, to the prevention of crime risks in the context of the identified risk activities. The company, by means of organizational charts or organizational communications adequately disclosed within it, defines:

- the delimitation of roles, the description of the tasks of each function and the related attributions and powers;
- the description of the fill lines.

The offences pursuant to Article 25-*bis* of Legislative Decree 231/2001
Counterfeiting of coins, public credit cards, stamped values and identification instruments or signs

Regulatory references:
- Counterfeiting of coins, spending and introduction into the State, subject to concert, of counterfeit coins (Art. 453 of the Criminal Code);
- Alteration of coins (Art. 454 of the Criminal Code);
- Spending and introduction into the State, without concert, of counterfeit coins (Art. 455 of the Criminal Code);
- Spending counterfeit coins received in good faith (Article 457 of the Criminal Code);
- Forgery of revenue stamps, introduction into the State, purchase, possession or putting into circulation of falsified revenue stamps (Article 459 of the Criminal Code);
- Counterfeiting of watermarked paper used for the manufacture of public credit cards or revenue stamps (Article 460 of the Criminal Code);
- Manufacture or possession of watermarks or instruments intended for the counterfeiting of coins, revenue stamps or watermarked paper (Article 461 of the Criminal Code);
- Use of counterfeit or altered revenue stamps (Art. 464 of the Criminal Code);
- Counterfeiting, alteration or use of trademarks or distinctive signs or patents, models and designs (Article 473 of the Criminal Code);
- Introduction into the state and trade of products with false signs (Article 474 of the Criminal Code);
- Undue use and falsification of credit and payment cards (Article 493-*ter* of the Criminal Code);
- Fraudulent transfer of values (Article 512-*bis* of the Criminal Code).

Sensitive Areas
Sensitive areas have been identified, within the organisational and corporate structure, i.e. those areas and business sectors with respect to which the risk of committing offences relating to counterfeiting of coins, public credit cards, revenue stamps and identification instruments or signs has been deemed to exist in the abstract. With reference to the offences listed above, the "sensitive areas" considered most specifically at risk of crime are the following:
- ✓ Management of financial transactions (collections and payments);
- ✓ Issuance, accounting and archiving of active invoices and credit notes;
- ✓ Checks on the regularity of active invoices;
- ✓ Settlement of benefits and collections;
- ✓ Verification and control of the inclusion of the clause relating to the obligation of traceability of financial flows in public contracts;
- ✓ Opening/closing of current accounts; reconciliation of bank statements and cash transactions; recording of receipts and payments in the general ledger;
- ✓ Cash management;
- ✓ Management of donations, donations, offerings and other liberal initiatives.
- ✓ Management of missions/transfers; management, control and authorization of expense reports; management and control of benefits and means provided; management of entertainment expenses and assets in representation.

Organizational control tools
All Recipients involved in sensitive areas and instrumental activities are required, as part of their activities, to comply with the rules of conduct, in accordance with the principles dictated by the Model and, in particular, by the Code of Ethics, specific control protocols and company procedures. In general, it is forbidden to:
a) engage in conduct such as to integrate the types of crime considered above;
b) requesting, soliciting, suggesting to employees and/or collaborators behaviors prohibited by the Model;
c) engage in conduct that, although it is such that it does not in itself constitute a crime falling within those considered above, can potentially become so;
d) put in place any situation of conflict of interest with regard to the Public Administration in relation to the provisions of the aforementioned offences.
e) carry out the behaviors indicated in the previous points both directly and through an intermediary.

The offences pursuant to Article 25-*bis*.1 of Legislative Decree 231/2001
Crimes against industry and commerce

Regulatory references:
- Disturbed freedom of industry or commerce (Article 513 of the Criminal Code);
- Unlawful competition with threat or violence (Article 513-*bis* of the Criminal Code);
- Fraud against national industries (Article 514 of the Criminal Code);
- Fraud in the exercise of trade (Article 515 of the Criminal Code);
- Sale of non-genuine foodstuffs as genuine (Art. 516 of the Criminal Code);
- Sale of industrial products with false signs (Art. 517 of the Criminal Code);
- Manufacture and trade of goods made by usurping industrial property rights (Article 517-*ter* of the Criminal Code);
- Counterfeiting of geographical indications or designations of origin of agri-food products (Article 517-*quater* of the Criminal Code).

Sensitive Areas
The following are the so-called Sensitive or Risk Areas identified with reference to crimes against industry and commerce:
- ✓ Sales/Proposal
- ✓ Integrated Supply Chain
- ✓ Quality & Welding

In consideration of the risk analysis carried out, the following crimes were found to be potentially feasible in the business context:
- ✓ access to information and/or trade secrets of competitors, including through the recognition or promise of money or other benefits to third parties, for the conception, design and implementation of new products for registration purposes;
- ✓ conception, design and construction of new products for registration purposes, usurping industrial property rights of others;
- ✓ failure to formulate remarks in the event of non-compliance and/or controls on the production, import and marketing processes of components in order to resell them to the customer, maliciously infringing inventions protected by patents;
- ✓ undue production and marketing of products in violation of licensing agreements by usurping industrial property rights of others.

Organizational system control tools
In order to prevent the crimes set out above, all recipients must comply, in addition to the principles of conduct already provided for and expressed in the Code of Ethics, also those set out in the organisational documents adopted by the company, as well as behave in accordance with the provisions of the law in force.
The general control measures are as follows:
- Code of Ethics;
- training on the Model and the issues referred to in Legislative Decree no. 231/2001, aimed at resources operating in the areas at risk;
- dissemination of the Model among the company's resources, through publication of the Model and the most significant protocols (e.g., Code of Ethics, Disciplinary System, Relevant Procedures, etc.) on the company intranet;
- dissemination of the Model among the Third Party Recipients required to comply with the relevant provisions (e.g. suppliers, contractors, consultants) by publishing it on the company's website;
- declaration by which the Recipients of the Model, including the Third Party Recipients (e.g. suppliers, consultants, contractors), undertake to comply with the provisions of the Decree;
- Disciplinary System aimed at sanctioning the violation of the Model and the Protocols connected to it;
- acquisition of a declaration, signed by each recipient of the Company's Model, of commitment to comply with it, including the Code of Ethics;
- creation of a "Section 231" within the intranet, where all the relevant documents within the Association's Model (e.g. Model, Code of Ethics, Protocols referred to therein) can be published.

The types of offences pursuant to Article 25-*ter* of Legislative Decree 231/2001
Corporate offences

Regulatory references:
- False corporate communications (Art. 2621 of the Italian Civil Code);
- False corporate communications by listed companies (Art. 2622 of the Italian Civil Code);
- Impeded control (Art. 2625 of the Italian Civil Code);
- Undue restitution of contributions (Art. 2626 of the Italian Civil Code);
- Unlawful distribution of profits and reserves (Art. 2627 of the Italian Civil Code);
- Unlawful transactions on the shares or quotas of the company or of the parent company (Art. 2628 of the Italian Civil Code);
- Transactions to the detriment of creditors (Art. 2629 of the Italian Civil Code);
- Failure to communicate the conflict of interest (Art. 2629-*bis* of the Italian Civil Code);
- Fictitious formation of capital (Art. 2632 of the Italian Civil Code);
- Undue distribution of company assets by liquidators (Art. 2633 of the Italian Civil Code);
- Corruption between private individuals (Art. 2635 of the Italian Civil Code);
- Incitement to corruption between private individuals (Art. 2635-*bis* of the Italian Civil Code);
- Ancillary penalties (Art. 2635-*ter* of the Italian Civil Code);
- Unlawful influence on the shareholders' meeting (Art. 2636 of the Italian Civil Code);
- Rigging (Art. 2637 of the Italian Civil Code);
- Obstruction of the exercise of the functions of public supervisory authorities (Art. 2638 of the Italian Civil Code);
- False or omitted declarations for the issuance of the preliminary certificate (Art. 54 of Legislative Decree no. 19 of 2 March 2023).

The aim of this Special Part is that all recipients conduct themselves in compliance with the provisions therein, in order to prevent the occurrence of the offences referred to in Art. 25-ter of the Decree which covers the majority of corporate crimes which currently constitute, together with market abuse, the only genuinely economic crimes for which the company can be held liable and which, since they are not occasioned by the exercise of the specific corporate activity, can be classified as general crimes.

Sensitive Areas

The Functions that are mainly sensitive to the offence pursuant to Article 25-*ter* of Legislative Decree 231/2001 are Finance, Treasury & Networking Capital and Controlling and Legal and Corporate Governance.

The legislation prohibits the following, among others, from being carried out:
- ✓ concealment of documents or other artifices in order to prevent and hinder statutory auditors, shareholders, auditors or members of control bodies in carrying out control activities;
- ✓ presentation of material facts that do not correspond to the truth or omission of information, the communication of which is required by law, on the economic, equity and financial situation of the company or group to which it belongs, misleading the recipients. Subjects active in these crimes may be directors, CFOs, persons in charge of preparing corporate accounting documents, auditors and liquidators. With regard to the activity in question, the offences in question may be committed during the process and activities preparatory to the approval of the draft financial statements and/or in the preparation of any corporate communication, for example by omitting information, or by reporting false or altered data in the documentation relating to the general accounting;
- ✓ determination of valuation items in the financial statements that do not comply with the real balance sheet, economic and financial situation of the company, in collaboration with the directors; presentation in the financial statements of other items that do not exist or whose value differs from the real value, or concealment of significant facts such as to change the representation of the actual economic conditions of the company;
- ✓ simulation or fraudulent arrangement of projects, prospectuses and documentation to be submitted for approval to the shareholders' meeting, even in competition with others;
- ✓ distribution of the company's assets among the shareholders before the payment of the company's creditors or the provision of the sums necessary to satisfy them, causing them damage;
- ✓ recognition or promise of money or other benefits to intermediaries as the price of their illicit mediation towards a public official, public service officer or one of the other subjects referred to in Art. 322-*bis* of the Criminal Code to obtain favours in the context of tax, judicial or extrajudicial proceedings;
- ✓ concealment of documents or other artifacts in order to prevent and hinder any checks and controls.

Organizational system control tools

This Special Section, in addition to the specific principles of conduct relating to the areas of risk indicated above, recalls the general principles of conduct provided for in this Model, which all directors and employees/collaborators of the company are required to observe.

In carrying out operations relating to corporate management, the following must be adopted and respected:
- the control protocols and company procedures, the documentation, the provisions relating to the hierarchical-functional organizational structure and the regulations in force;
- the rules relating to the administrative, accounting, financial and management control system of the company;
- the Organizational Model.

The Model provides for the express prohibition of:

- to carry out, collaborate or cause the adoption of conduct that – considered individually or collectively – integrates, directly or indirectly, the types of crime falling within those considered above (Article 25-*ter* of the Decree);
- engage in conduct that, although it is such that it does not in itself constitute a crime falling within those considered above, can potentially become so, as it is suitable and unequivocally directed to their commission;
- violate the company principles and procedures that are integral parts of the Model itself.

The types of offences pursuant to Article 25-*quater of Legislative Decree 231/2001*
Offences with the purpose of terrorism or subversion of the democratic order provided for by the Criminal Code and special laws

Regulatory references:
- Subversive associations (Art. 270 of the Criminal Code);
- Associations with the purpose of terrorism, including international terrorism, or subversion of the democratic system (Art. 270-*bis* of the Criminal Code);
- Aggravating and mitigating circumstances (Art. 270-*bis*.1 of the Criminal Code);
- Assistance to members (Art. 270-*ter* of the Criminal Code);
- Enlistment for the purpose of terrorism, including international terrorism (Art. 270-*quater* of the Criminal Code);
- Organization of transfers for terrorist purposes (Art. 270-*quater*.1 of the Criminal Code);
- Training for activities with the purpose of terrorism, including international terrorism (Art. 270-*quinquies* of the Criminal Code);
- Financing of conduct for terrorist purposes (Art. 270-*quinquies*.1 of the Criminal Code);
- Theft of seized goods or money (Art. 270-*quinquies*.2 of the Criminal Code);
- Possession of material for terrorist purposes (art. 270-quinquies.3 Criminal Code);
- Conduct for the purpose of terrorism (Art. 270-*sexies* of the Criminal Code);
- Attack for terrorist or subversion purposes (Article 280 of the Criminal Code);
- Act of terrorism with deadly or explosive devices (Article 280-*bis* of the Criminal Code);
- Act of nuclear terrorism (Article 280-*ter* of the Criminal Code);
- Kidnapping for the purpose of terrorism or subversion (Article 289-*bis* of the Criminal Code);
- Kidnapping for the purpose of coercion (Article 289-*ter* of the Criminal Code);
- Art. 302 of the Criminal Code which governs the instigation of one of the crimes indicated herein;
- Political conspiracy by agreements (Article 304 of the Criminal Code);
- Political conspiracy by association (Article 305 of the Criminal Code);
- Armed band: formation and participation (Art. 306 of the Criminal Code);
- Association with participants in conspiracy or armed gang (Article 307 of the Criminal Code);
- Manufacture or possession of explosive materials (art. 435 of the Criminal Code);
- Seizure, hijacking and destruction of an aircraft or damage to ground installations (Articles 1 and 2 of Law 342/1976).

Attention should also be paid to the cases referred to in Art. 272 of the Criminal Code (subversive or anti-national propaganda and apology), 280 of the Criminal Code (attack for terrorist purposes or subversion), 284 of the Criminal Code (armed insurrection against the powers of the State), 289-*bis* of the Criminal Code (kidnapping for the purpose of terrorism or subversion).
The analysis of the business processes has made it possible to identify the activities in which the types of offences referred to in Article 25-*quater* of Legislative Decree 231/2001 (Crimes Financing of terrorism) could be carried out in the abstract.

Sensitive areas
The following are the so-called Sensitive or Risk Areas identified with reference to terrorist financing offences:
- ✓ Finance, Treasury & Networking Capital and Controlling
- ✓ Sales/Proposal
- ✓ Integrated Supply Chain
- ✓ Client & Field Service

By way of example, and not exhaustively, the following activities have been identified:
- ✓ operations of an extraordinary nature, through the improper management of the role held by the Company, in order to promote, finance, establish, organize, or participate in associations, both national and transnational, also aimed at terrorist activities or subversion of the democratic order and also in the event of cooperation of members of the Company with two or more subjects for the prosecution of any non-culpable crime;
- ✓ the conclusion of contracts to carry out works for customers linked to associations with terrorist purposes, facilitating their activities;
- ✓ the conclusion of contracts for the supply of goods or labour with suppliers linked to terrorist associations (e.g. through false or inflated invoices the company could transfer financial resources to finance terrorist activities).

Organizational system control tools
For each of the sensitive activities identified, the control systems and safeguards in place to mitigate risks with reference to crimes with the purpose of terrorism or subversion of the democratic order have been identified:
- the Company guarantees the compliance of operations with the provisions in force on anti-terrorism/anti-money laundering, using specific applications capable of consulting the data of names suspected of terrorist financing;
- the offices in charge, in accordance with the provisions of the law in force and the role played in relations with suppliers and/or customers, prepare and consult the anti-terrorism lists prepared by the official bodies;
- automatic checks on the names suspected of terrorism and countries with which it is prohibited by law to operate (Black List);
- the company prohibits the conclusion of contracts or the opening of new relationships in favour of subjects – natural or legal persons – whose names are contained in the Anti-Terrorism Lists;
- traceability of activities both at the level of the IT system and in terms of documentation;
- provide for the assignment of responsibilities with regard to the management of potentially suspicious terrorist financing transactions;

- prevention protocols, procedures and Code of Ethics.

The offences pursuant to Article 25-quinquies of Legislative Decree 231/2001
Crimes against the individual personality

Regulatory references:
- Reduction or maintenance in slavery or servitude (Article 600 of the Criminal Code);
- Child prostitution (Art. 600-*bis* of the Criminal Code);
- Child pornography (Art. 600-*ter* of the Criminal Code);
- Possession of pornographic material (Art. 600-*quater* Criminal Code);
- Virtual pornography (Art. 600-*quater*1 Criminal Code);
- Tourist initiatives aimed at the exploitation of child prostitution (Art. 600-*quinquies* Criminal Code);
- Trafficking in persons (Article 601 of the Criminal Code);
- Trafficking in organs removed from living persons (Art. 601-*bis* c.p.);
- Purchase and alienation of slaves (Article 602 of the Criminal Code);
- Illegal intermediation and exploitation of labour (Art. 603-*bis* Criminal Code);
- Solicitation of minors (Art. 609-*undecies* of the Criminal Code);
- Torture (Art. 613-*bis* of the Criminal Code);
- Instigation of a public official to commit torture (Art. 613-*ter* of the Criminal Code);

Sensitive Areas
Sensitive activities identified:
1) selection of suppliers;
2) relations with contractors;
3) selection of partners;
4) relations with third parties that imply the use by the Entity of labour belonging to the same third parties.

Conceivable crimes:
- Employment of illegally staying third-country nationals;
- Reduction or maintenance in slavery or servitude;
- Illegal intermediation and exploitation of labour.

Organizational system control tools
In the areas "at risk of crime" considered, there are the following General Control Units (to which are added Specific Control Controls in relation to individual sensitive activities or categories of sensitive activities):
1) Code of Ethics;
2) training on the Model and the issues referred to in Legislative Decree no. 231/2001, aimed at resources operating in areas at risk, with training methods specifically planned in consideration of the role played;
3) dissemination of the Model among internal resources, by delivering a copy on documentary or electronic support and publication of the Model and the most significant protocols (e.g., Code of Ethics, Disciplinary System, Relevant Procedures, etc.) on the company intranet;
4) dissemination of the Model among the Third Party Recipients required to comply with the relevant provisions (e.g., suppliers, contractors, consultants) by publishing it on the company's website or making it available in paper or electronic format;
5) declaration by which the Recipients of the Model, including the Third Party Recipients (e.g., suppliers, consultants, contractors), undertake to comply with the provisions of the Decree;
6) Disciplinary System aimed at sanctioning the violation of the Model and the Protocols connected to it, including that provided for by the applicable CCNL;
7) acquisition of a declaration, signed by each recipient of the Model of commitment to compliance with the same, including the Code of Ethics;
8) creation of a "Section 231" within the intranet, where all the relevant documents within the Model (e.g. Model, Code of Ethics, Internal Protocols where referred to) can be published.

The offences pursuant to Article 25-*septies* of Legislative Decree 231/2001
Crimes of manslaughter or serious or very serious injuries committed with violation of the rules on the protection of health and safety at work

Regulatory references:
- The crime of manslaughter (Art. 589, Criminal Code);
- The crime of serious or very serious culpable injuries (Art. 590, Criminal Code);
- Sanctions for the employer and the manager (Art. 55, Legislative Decree n. 81 of April 9, 2008).

The sensitive activities identified, with reference to the crime of manslaughter or serious or very serious injuries committed with violation of the rules on the protection of health and safety at work referred to in Art. 25 *septies* of Legislative Decree 231/2001, are all areas and business processes with the presence of risk factors, as identified in the Risk Assessment Document pursuant to Legislative Decree 81/2008 as amended.

Sensitive areas
The following is a list of the so-called sensitive or risk areas identified with reference to the crimes of manslaughter, or serious or very serious injuries committed in violation of the rules on the protection of health and safety at work:
- ✓ HSE Department (Health, Safety, Environment) – RSPP – Employer – D.D.L. and Managers in charge.

The following include, but are not limited to, activities at risk:
- ✓ violation or omissions, lack of diligence, imprudence or inexperience, on the part of the Company, in the fulfilment of the obligations deriving from accident prevention regulations and on the protection of hygiene and health at work (e.g. failure to carry out risk assessment, control, prevention, training, protection, preparation of document flows provided for by law, etc.) that may involve the offence of manslaughter or culpable injury in the event of a serious accident or very serious of employees or collaborators;
- ✓ Lack of/incorrect definition of the system of powers of attorney/delegations/appointments in the field of health and safety in the workplace: RSPP – ASPP – RLS – Emergency management officers (emergencies, fire, first aid) – Doctor;
- ✓ competent – Employer's delegate – Employer's deputy delegate;
- ✓ Failure to adopt/incomplete adoption of the documentation on safety and health in the workplace required by legislation and in OSH; e.g.: risk assessment document (DVR), emergency management instructions, first aid instructions, evacuation instructions, health surveillance instructions, safety signs;
- ✓ Failure to carry out periodic checks on compliance with the requirements on safety and health in the workplace provided for by legislation and in the OSH, including periodic health visits.

Organizational system control tools
The company has adopted an Occupational Safety System (OSH), which regulates obligations and procedures regarding health and safety at work, identifying roles and responsibilities, specifically:
- Organisational model for the application of Legislative Decree 81/08 on health and safety in the workplace;
- company guidelines for the management of emergencies and safety signs;
- company guidelines for the management of information, training and communication on health and safety in the workplace, such as to guarantee at all company levels useful knowledge for the identification, reduction and management of risks in the workplace;
- company guidelines for the management of plants, machines, equipment, substances and personal protective equipment;
- company guidelines for the management of health surveillance;
- company guidelines for the management of safety measures in contracts for works, services and supplies, including aspects concerning the costs of safety in contracts;
- procedure for monitoring and updating the Occupational Safety System (OSH);
- guidelines for risk assessment, which describes the methodology for the correct execution and management of risk assessment, as well as for the execution and updating/verification of risk assessment and the drafting of the related risk assessment documents (DVR);
- internal procedures, 231 protocols and Code of Ethics.

The offences pursuant to Article 25-*octies* of Legislative Decree 231/2001
Crimes of receiving stolen goods, laundering and use of money, goods or utilities of illegal origin, as well as self-laundering

Regulatory references:
- Receiving stolen goods (Article 648 of the Criminal Code);
- Money laundering (Article 648-*bis* of the Criminal Code);
- Use of money, goods or utilities of illicit origin (Article 648-*ter* of the Criminal Code);
- Self-laundering (Art. 648-*ter* 1 of the Criminal Code).

The Italian legislation on the prevention of money laundering crimes provides for rules aimed at hindering money laundering practices, prohibiting, among other things, the carrying out of transfer transactions of significant amounts with anonymous instruments and ensuring the reconstruction of transactions through the identification and due diligence of customers and the registration of data in special archives.
Specifically, the body of legislation on money laundering is constituted first of all by the Anti-Money Laundering Decree, which partly repealed and replaced Law 197/1991.

Sensitive areas
As part of the *Risk Assessment*, carried out by the competent internal structures and updated annually, also through interviews with the resources of the Divisions/Areas concerned who are aware of the specific area analysed, all the activities at risk of crime relating to this special part and referring to macro-processes and business processes are identified. Following an in-depth analysis of its corporate reality, the main Sensitive Activities that the company has identified within itself are the following:
- ✓ Finance, Treasury & Networking Capital and Controlling
- ✓ Sales/Proposal
- ✓ People & Culture / HR Administration
- ✓ Legal and Corporate Governance
- ✓ Integrated Supply Chain
- ✓ Quality & Welding
- ✓ Client & Field Service

In relation to the described Sensitive Activities – all of which can be theoretically hypothesized – some corporate bodies and functions are considered to be particularly involved.
The following include, but are not limited to, activities at risk:
- ✓ extraordinary and Merger & Acquisition transactions carried out through proceeds deriving from the commission or participation in non-culpable crimes, with conduct aimed at concretely hindering the identification of the criminal origin of the resources used;
- ✓ with regard to this type of activity, the crimes of money laundering or use of money or other benefits could occur in the interest and/or to the advantage of the Company through sales to new customers whose corporate purpose is difficult to ascertain, to know the economic profile and to verify over time the ownership of the business relationship (for example, in the case of continuous changes in the corporate structure);
- ✓ violation of the current legislation on anti-money laundering carried out through improper management of the role held in the company in order to establish/mediate contractual relationships aimed at replacing, transferring money, goods, other utilities of illegal origin, or to implement a series of actions aimed at making it difficult to identify their origin, with particular but not exclusive reference to transactions with so-called "blacklist" countries;
- ✓ use of money from illegal activities (e.g. crimes committed in the context of the company's tax returns) for the payment of expense reports;
- ✓ evasion of income or value added taxes through the use of invoices for (even partially) non-existent transactions and use of the resources thus obtained to make a donation;
- ✓ selection process of the supplier/contractor in order to generate an economic benefit for the company (e.g. more competitive purchase price), through the import of counterfeit and/or altered goods/products.

Organizational system control tools
This Special Section refers to conduct carried out by directors, managers, employees as well as external collaborators and partners of the company, including any persons belonging to other companies involved in the management of the areas of activity at risk, and in any case of those who, even if only de facto, fall within the categories of top management or subordinates of the company.
It was considered that, for the prevention of these crimes, the following can perform an adequate preventive function:
- specific prevention protocols that are an integral part of the Organisation, Management and Control Model pursuant to Legislative Decree 231/01 adopted by the company;
- the principles set out in the Code of Ethics;
- corporate procedures that are an integral part of the Sofinter Group's Corporate Compliance Program;
- traceability and ex-post verifiability of transactions through adequate documentary/IT supports;
- segregation of tasks (application of the principle of separation of activities between those who authorise, those who execute and those who control);
- existence of a system of delegations consistent with the organizational responsibilities assigned (there must be formalized rules for the exercise of powers of signature and internal authorization powers).

The types of offences pursuant to Article 25-*octies.*1 of Legislative Decree 231/2001
Offences relating to non-cash payment instruments

Regulatory references:
- Improper use and falsification of payment instruments other than cash (Article 493-*ter* of the Criminal Code);
- Possession and dissemination of equipment, devices or computer programs aimed at committing crimes concerning payment instruments other than cash (Article 493-*quater* of the Criminal Code);
- Fraudulent transfer of values (Article 512-*bis* of the Criminal Code);
- Computer fraud (Art. 640-*ter* of the Criminal Code).

Sensitive areas
The cases referred to in Art. 25 *octies*-1 could be relevant with reference to the collection of sales that require the use of payment instruments other than cash, such as online sales, payments with the use of devices that allow the use of electronic money, prepaid, debit or credit cards.
In addition, the scope of the Directive relates not only to means of payment other than so-called "traditional" cash, but also to virtual money and related payments using electronic money, virtual currency and mobile phone payments.
The Functions that are mainly sensitive to the offence pursuant to Article 25 octies-1 are as follows:
- Finance, Treasury & Networking Capital and Controlling.

The sensitive activities identified are the following:
- ✓ Company personnel, having received counterfeit or cloned credit or payment cards, use them by carrying out transactions relating to travel expenses;
- ✓ Activity instrumental to the commission of the crimes of corruption / undue inducement to give or promise benefits / trafficking in illicit influence. Outgoing monetary and financial flows with the aim of fulfilling the obligations of various kinds contracted by the company could constitute support for the establishment of financial resources – both in Italy and abroad – that can be allocated to the Public Official, Public Service Officer or Private Entity.

Organizational system control tools
With reference to crimes relating to payment instruments other than cash, please refer to the control principles reported in Computer crimes and crimes against the Public Administration.
In addition to the general rules of conduct, the following are additional operational control measures to prevent the commission of crimes relating to non-cash payment instruments, with particular reference to processes instrumental to the commission of crimes such as the management of monetary and financial flows:
- each cash movement must be authorized by persons with appropriate powers and supported by appropriate documentation;
- credit cards draw on the company's current account and can only be used for so-called "construction site expenses". The company does not allow the mixed use of credit cards, which are provided with the name of the employee to whom they are assigned;
- payments are made through tools that ensure traceability (e.g. bank transfers, etc.) and, only on a residual basis and subject to authorization, through the use of cash in compliance with the limits provided for by the laws in force;
- payments must always be made to the person who provided the good and/or service, with the obligation to carry out specific checks on the identity of third parties;
- transactions involving the use or use of economic or financial resources must always have an express reason and must be documented and recorded in accordance with the principles of accounting correctness and transparency;
- the company's receipts and payments, as well as the flows of money, must always be traceable and documentable;
- the verification of the regularity of payments is envisaged, also with reference to the coincidence between the recipient/payer and the counterparty actually involved in the transaction and the control of the correctness of the company's financial flows with reference to payments to third parties;
- for the management of incoming and outgoing flows, only banking channels and those of other accredited financial intermediaries subject to European Union regulations or credit/financial institutions located in a non-EU country that imposes obligations equivalent to those provided for by money laundering laws and provides for the control of compliance with these obligations are used;
- formal and substantial controls are carried out and constant monitoring of the company's financial flows, with reference to payments to third parties, taking into account the registered office of the counterparty company, the credit institutions used, any corporate screens and trust structures used for extraordinary transactions or operations;
- the company ensures the tracking of the number of credit cards assigned to employees by tracing them back from the current account in its name;
- it is forbidden to use current accounts anonymously or with fictitious names, neither in Italy nor in other foreign countries;
- the holders of electronic and/or digital signatures are identified on the basis of contractual regulations with the Certification Authorities issuing the signatures; the custody and use of electronic and/or digital signature devices are entrusted to the holders of the same and must comply with the contractual regulations with the Certification Authorities issuing the signatures.

Crimes under Article 25-octies.2 of Legislative Decree 231/2001
Crimes relating to the violation of European Union restrictive measures [Article added by Legislative Decree no. 211 of 30/12/2025]

Regulatory references:
- Violation of European Union restrictive measures (Article 275-bis of the Criminal Code);
- Violation of disclosure obligations imposed by a European Union restrictive measure (Article 275-ter of the Criminal Code);
- Violation of the conditions of the authorization to carry out activities (Article 275-quater of the Criminal Code);
- Negligent violation of European Union restrictive measures (Article 275-quinquies of the Criminal Code)

Sensitive Areas
Risk areas concern processes impacting exports, imports, international transactions, disclosure obligations, and relationships with sanctioned entities.
- **Export / International Trade Area**

Risks:
✓ export or re-export of goods to sanctioned countries or entities (Russia, Belarus, Iran, Syria, etc.);
✓ sale of dual-use goods without authorization;
✓ contracts with entities not officially sanctioned but controlled by designated entities → circumvention offense.
- **Purchasing and Supply Chain Area**

Plants often include parts produced or integrated through:
✓ foreign suppliers,
✓ subcontractors,
✓ distributors.
The chain may conceal sanctioned entities or prohibited final destinations, including through triangulation. Risk: Indirect circumvention of EU sanctions through countries not subject to restrictions but used as "shields".
- **Design and technical assistance for systems in sanctioned countries**

EU restrictive measures affect not only tangible assets, but also:
✓ engineering services,
✓ technical assistance,
✓ consultancy for design, installation, and maintenance.
Providing technical assistance to sanctioned entities is prohibited. Risk: this may constitute "provision of prohibited services", even without transferring assets.
- **International payments and project financing**

System engineering companies often operate through:
✓ advances,
✓ letters of credit,
✓ escrow accounts,
✓ structured financing.
Restrictive measures may prohibit financial transactions with certain entities. Risk: movement of funds on behalf of or for the benefit of sanctioned entities (imprisonment + fine).
- **Ignorance or failure to comply with disclosure requirements**

In the system engineering sector, it is typical to manage:
✓ goods in transit,
✓ temporary storage,
✓ customs warehouses,
✓ funds for foreign procurement.
Risk: liability for failure to disclose, even inadvertently.
- **Management of technical and commercial documentation**

In the plant engineering sector, documentation includes:
✓ technical data sheets,
✓ manuals,
✓ certificates of conformity,
✓ end-use declarations.
Risk: inaccurate documentation may constitute evasive conduct.

Organizational system control tools
1) Screening and verification of counterparties
Screening is considered one of the most important mechanisms for avoiding:
• relationships with designated parties,
• prohibited transactions,
• circumvention through front companies or third-party countries.
Operational tools:
• automated checks against EU (consolidated list), UN, OFAC, and UK HMT lists;
• beneficial owner verification to prevent intermediaries;
• continuous monitoring (not just at the time of signing).

2) Controls on goods, technologies, and services

The decree highlights the need to control goods and services with a risk of strategic importance, in particular:

- dual use,
- military products,
- restricted technological components,
- technical assistance services.

Tools:

- goods classification (customs codes, ECCN, dual use);
- verification of EU and national authorizations;
- embargo check for countries subject to restrictive measures;
- automatic export blocking in the absence of clearance.

3) Control of financial transactions

Tools:

- filters on international payments to banks/institutions affected by restrictions;
- checks on letters of credit, escrow accounts, project financing;
- automatic blocking of suspicious payments;
- review of the transaction approval workflow.

4) Document flow control

Tools:

- digital and traceable management of all export and contractual documentation;
- verification of end-use (EUC – End Use Certificate);
- formal and substantive checks on: invoices, bills of lading, contracts, technical data sheets.

5) Supply Chain and Third-Party Country Monitoring

Tools:

- verification of subcontractors and suppliers;
- verification of the actual country of origin/destination of goods;
- periodic audits of at-risk suppliers;
- insertion of sanctions-compliant contractual clauses.

6) Information requirements and internal reporting procedures

Tools:

- internal reporting procedures to authorities (MEF, Bank of Italy, ADM);
- clear information flows between company functions;
- specific whistleblowing channels for EU sanctions.

The offences pursuant to Article 25-*novies* of Legislative Decree 231/2001
Copyright offences

Regulatory references:

- Making a protected intellectual work or part thereof available to the public - Crimes committed against another's work not intended for publication if the work's honor/reputation is damaged (Article 171 of Law No. 633 of April 22, 1941);
- Unauthorized publication on media not marked pursuant to Law No. 166/2024 - Reproduction or transfer of database content to another media (Article 171-*bis* of Law No. 633 of April 22, 1941);
- Unauthorized duplication of intellectual works intended for television, cinema, etc. (Article 171-*ter* of Law No. 633 of April 22, 1941);
- Failure to provide identification data for media pursuant to Law No. 166/2024 (Article 171-*septies* of Law No. 633 of April 22, 1941);
- Fraudulent production, sale, or import of decoding equipment (Article 171-*octies* of Law No. 633 of April 22, 1941);
- Unauthorized use, duplication, or reproduction of protected works or materials (Article 174-*ter* of Law No. 633 of April 22, 1941);
- Reporting and notification obligations (Article 174-*sexies* of Law No. 633 of April 22, 1941);
- Agreements between SIAE, other collective management organizations, and independent management entities (Article 181-*bis* of Law No. 633 of April 22, 1941).

Sensitive Areas

The sensitive activities identified, with reference to the crimes relating to copyright infringement referred to in Article 25 *nonies* of Legislative Decree 231/2001, are the following:

- ✓ Use of resources and information of an IT or telematic nature, or of any other intellectual work protected by copyright (with particular reference to the occasions of crime "Management of activities related to the purchase and use of software, databases or any other intellectual work protected by copyright" and "Management of activities related to the implementation and/or updating of the website and, more generally, use of the company telematic network");
- ✓ Management of the company's presentation activities to the public;
- ✓ Improper use of works or parts of works (e.g. graphics, literature, etc.) protected by copyright;
- ✓ Misuse, for example in the course of a conference or other public presentation, of works or parts of works protected by copyright;
- ✓ Use of software, databases or other intellectual works in the absence of a suitable or valid license/authorization from the owner of the relevant rights;
- ✓ Abusive, fraudulent or otherwise improper management of other people's works or parts of them, through their publication on the website or in any case their dissemination through the company's telematic network.

Organizational system control tools

For operations concerning the management of servers, websites, social networks and internal/external dissemination of news, the management of information covered by copyright/intellectual property, the management of the acquisition and development of equipment, devices (including detection) or computer programs and installation, maintenance, connection or other services relating to hardware, related software and networks, technical components connected with the system, the protocols/procedures provide that:

- the works/information protected by copyright/intellectual property acquired by the company for the purposes of the company's activities are catalogued in a special database;
- for the works/information for which the licenses have been acquired, the database also includes the following data: (i) date of purchase of the license; (ii) the date of expiration of the license; (iii) type of use authorized by the license agreement (e.g. upload to the website, public dissemination, use for brochures and their maximum number of copies that can be used, etc.);
- policies and methods are defined and activated to control access by users to content download sites;
- controls are provided by the competent Department/Office on activities involving the use of works/information protected by copyright/intellectual property;
- the criteria and methods for the management of software systems are defined, which must provide for the compilation and maintenance of an updated inventory of the software in use by the company;
- criteria and procedures are defined and activated to check that the purchase and use of software and other works/information protected by copyright/intellectual property are formally authorized and certified;
- periodic checks are carried out on the installed software and on the mass memory of the systems in use in order to check for the presence of prohibited and/or unlicensed and/or potentially harmful software;
- the applications keep track of changes to data and systems made by users (if the management of this activity is outsourced, the contracts that govern the relationship with the service providers provide for specific clauses that require, for the software suppliers, the compliance of the software supplied with the laws and regulations in force and the indemnity for the company in the event of violations committed by the service providers themselves).

The offences pursuant to Article 25-*decies* of Legislative Decree 231/2001
Inducement not to make statements or to make false statements to the judicial authority

Regulatory references:
- Inducement not to make statements or to make false statements to the judicial authority (Article 377-*bis* of the Criminal Code).

The analysis of the company's processes has made it possible to identify the following "sensitive" activities, in the context of which the crime in question could theoretically take place:
- ✓ Management of relations with the Judicial Authority;
- ✓ Management of consultancy and professional services;
- ✓ Management of any judicial and extrajudicial disputes.

Sensitive Areas
The Functions mainly sensitive to the commission of the offence pursuant to Article 25-*decies* of Legislative Decree 231/2001 are People & Culture/HR Administration and Legal and Corporate Governance.
The legislation prohibits the following behaviors:
- ✓ use violence or threats, carry out acts of intimidation or offer or promise money or other benefits in order to induce a person called upon to make statements before the judicial authorities, not to make such statements or to make false statements.

Organizational system control tools
For the purposes of implementing the rules of conduct in accordance with the provisions of Legislative Decree 231, the Recipients of this Special Part of the Model, in addition to complying with the provisions of the law on the subject, the rules in the Code of Ethics and the principles indicated in the General Part of this Model, must comply with the behavioural protocols, placed to protect the risks of crime identified above and referable to the activities at risk.
Reference is also made to the provisions of the Code of Ethics and to the procedures and protocols with regard to the specific principles of conduct and existing control standards regarding:
- Management of consultancy and professional services
- management of any judicial and extrajudicial disputes.

The types of offences pursuant to Article 25-*undecies* of Legislative Decree 231/2001
Environmental crimes

Regulatory references:
- Environmental pollution (Article 452-*bis* of the Criminal Code);
- Trade of polluting products (Art. 452-bis.1 Criminal Code);
- Death or injuries as a consequence of the crime of environmental pollution and trade of polluting products (Art. 452-ter Penal Code);
- Environmental disaster (Article 452-*quater* of the Criminal Code);
- Culpable crimes against the environment (Article 452-*quinquies* of the Criminal Code);
- Trafficking and abandonment of highly radioactive material (Article 452-*sexies* of the Criminal Code);
- Obstruction of control (Article 452-*septies* of the Criminal Code);
- Aggravating circumstances (Article 452-*octies* of the Criminal Code);
- Failure to remediate (Article 452-*terdecies* of the Criminal Code);
- Organised activities for the illegal trafficking of waste (Article 452-quaterdecies of the Criminal Code);
- Concept of abusiveness (Art. 452-quinquiesdecies);
- Aggravating circumstances (Art. 452-sexiesdecies);
- Killing, destruction, capture, removal, possession of specimens of protected wild animal or plant species (Article 727-*bis* of the Criminal Code);
- Destruction or deterioration of habitats within a protected site (Article 733-*bis* of the Criminal Code) - REPEALED by Legislative Decree no. 81 of 21 April 2026;
- Environmental Code – Legislative Decree 152/06;
- Law no. 150 of 7 February 1992;
- Law no. 549 of 28 December 1993 – Measures to protect stratospheric ozone and the environment;
- Legislative Decree no. 202 of 6 November 2007 – Implementation of Directive 2005/35/EC on pollution caused by ships and consequent sanctions.

Sensitive Areas
This Special Section refers to the environmental crimes referred to in Article 25 *undecies* of Legislative Decree 231/2001 and in particular identifies the so-called "sensitive" activities (those where the commission of the crime is theoretically possible and which have been identified as part of the risk assessment activity), specifying the principles of conduct and operational controls for the organisation, performance and management of the operations carried out in the context of the aforementioned "sensitive" activities.
The following are the Sensitive or Risk Areas identified with reference to environmental crimes:
- ✓ HSE Department (Health, Safety, Environment) – General Services – Maintenance Technicians

In consideration of the risk analysis carried out, the following crimes were found to be potentially feasible in the business context:
- ✓ absence or poor maintenance of the purifier that involves discharges beyond the limits;
- ✓ incorrect management of operational activities (e.g. dosage of chemicals in production) which generates an exceedance of the limits in wastewater;
- ✓ spillage of hazardous chemicals into the water network that results in the authorized limits being exceeded;
- ✓ violation and/or lack of controls of the provisions of the authorization;
- ✓ construction and management of unauthorised/suspended/revoked discharges (discharges of industrial wastewater Art. 137 paragraphs 2, 3, 5, 11 and 13 of Legislative Decree 152/06; discharges of hazardous substances Art. 108 of Legislative Decree 152/06);
- ✓ false indication of the nature, composition and chemical-physical characteristics of the waste in the preparation of the waste analysis certificate, or use of a false certificate of analysis during the transport of non-hazardous own waste (illegal waste trafficking Art. 259 Legislative Decree 152/2006; violation of the obligations of communication, keeping of mandatory registers and forms Legislative Decree 152/06, Art. 258, paragraph 4);
- ✓ storage areas that are not adequately paved/waterproofed (environmental pollution under Article 452-*bis* of the Criminal Code);
- ✓ incorrect management/maintenance of production plants, conduct of activities in non-compliance with the authorisation requirements/lack of controls (prevention and limitation of emissions into the atmosphere Legislative Decree no. 152/06, Art. 279, paragraph 5; environmental pollution Art. 452-*bis* of the Criminal Code);
- ✓ violation of the prohibition on the use of substances harmful to stratospheric ozone (cessation and reduction of the use of substances harmful to the stratospheric ozone (cessation and reduction of the use of substances harmful to the stratospheric ozone); environmental pollution Art. 452-*bis* of the Criminal Code).

Organizational system control tools
In line with the corporate ethical principles referred to in the General Part of the Organisational Model pursuant to Legislative Decree 231/2001 of the Code of Ethics, in carrying out the sensitive activities mentioned above, all the Recipients of the Model are required to observe the following principles of conduct and control: adopt prudent, correct, transparent and collaborative behaviour for the protection of the environment, in accordance with their training and experience, as well as the instructions and means provided or prepared by the company. In general, it is required to:
- comply with the legislation for the purpose of protecting the environment, in particular by exercising all appropriate controls and activities suitable for safeguarding the environment itself;
- correctly use equipment and other work equipment in order to avoid environmental problems;

- to act directly, in the face of a detected danger and only in cases of urgency, compatibly with their skills and possibilities;
- carry out waste management and disposal activities with the lowest possible environmental impact;
- obligations regarding the health and safety of workers (pursuant to Legislative Decree 81/2008) and environmental legislation;
- procedures and Code of Ethics.

The offences pursuant to Article 25-*duodecies* of Legislative Decree 231/2001
Offences involving the use of illegally staying third-country nationals

Regulatory references:
- Legislative Decree no. 286 of 25 July 1998 – "Consolidated text of the provisions concerning the regulation of immigration and rules on the condition of foreigners".

This crime consists of the conduct of those who, as an employer, employ foreign workers without a residence permit, or whose permit has expired and whose renewal has not been requested within the terms of the law, or is revoked or cancelled if the workers employed are (alternatively):
- more than three in number;
- children of non-working age;
- subject to the other particularly exploitative working conditions referred to in the third paragraph of Art. 603-*bis* of the Criminal Code, i.e. exposed to situations of serious danger, with reference to the services to be performed and working conditions.

Sensitive Areas
- People & Culture/HR Administration
- Integrated Supply Chain

The sensitive activities identified, with reference to the crimes referred to in Art. 25-*duodecies* of Legislative Decree 231/2001, are the following:
- ✓ Selection and recruitment of personnel: employment of foreign workers without a residence permit or with an expired permit whose renewal has not been requested, within the terms of the law, or with a permit revoked or cancelled;
- ✓ Choice of supplier/contractor: choice of suppliers who do not ensure adequate protection for their employees or who employ foreign workers without a residence permit or with an expired permit whose renewal has not been requested, within the terms of the law, or with a permit revoked or cancelled;
- ✓ Choice of supplier/contractor: choice of suppliers who subject workers to conditions of particular exploitation or keep them in a state of continuous subjection.

Organizational system control tools
This Special Part provides for the express prohibition on the company (and the Recipients, Employees, and Consultants/Partners to the extent necessary for the functions they perform) to:
- engage, collaborate or cause the performance of conduct such that, taken individually or collectively, integrates, directly or indirectly, the types of crime falling within those considered above;
- violate the principles and procedures existing in the company and/or provided for in this Special Section.

Specifically, it is absolutely forbidden to:
1. Hire or otherwise employ foreign workers without a regular residence permit;
2. Hire or otherwise employ foreign workers whose residence permit has expired and whose renewal has not been requested within the terms of the law;
3. Hire or otherwise employ foreign workers whose residence permit has been revoked or cancelled.

For the purposes of implementing the rules listed, in addition to the general principles contained in the General Part of the Model and in the Code of Ethics, control protocols and specific company procedures must also be respected.

The offences pursuant to Article 25-*quinquiesdecies* of Legislative Decree 231/2001
Tax crimes

Regulatory references:
- Fraudulent declaration through the use of invoices or other documents for non-existent transactions (Article 2, Legislative Decree no. 74/2000);
- Fraudulent declaration by other artifices (Article 3, Legislative Decree 74/2000);
- Issuance of invoices or other documents for non-existent transactions (Article 8, paragraphs 1 and 2 *bis*, Legislative Decree 74/2000);
- Concealment or destruction of accounting documents (Article 10, Legislative Decree 74/2000);
- Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000);
- Unfaithful declaration (Article 4, Legislative Decree 74/2000);
- Failure to declare (Article 5, Legislative Decree 74/2000);
- Undue compensation (Article 10 *quater*, Legislative Decree No. 74/2000).

Sensitive Areas
The risk assessment activities carried out identified the following "sensitive" activities for the crimes indicated above, i.e. those business processes for which the risk of committing the crimes in question was considered to exist in the abstract:
- Finance, Treasury & Networking Capital and Controlling.

The recipients of this Special Section are the directors, the head of the function responsible for preparing the company's financial reports and related tax documentation, the statutory auditors, the auditors, as well as the employees subject to supervision and control by the top management in the areas of activity at risk. The sensitive activities identified, with reference to the tax crimes referred to in Art. 25 *quinquiesdecies* of Legislative Decree 231/2001, are as follows:

1. Tax management:
   - fraudulent declaration through the use of invoices or other documents for non-existent transactions, for example for the purpose of obtaining tax savings;
   - fraudulent declaration through other artifices, such as false documents aimed at tax evasion;
   - issuing invoices or other documents for non-existent transactions, so as to allow other companies to evade taxes;
   - concealment or destruction of accounting documents, in such a way as to make it impossible to effectively reconstruct the company's turnover;
   - fraudulent evasion of tax payments, exemplified by the dispersion of corporate assets capable of generating fraudulent savings for the company.
2. Finance:
   - the company records invoices in the accounts for (even partially) non-existent transactions, to be used in order to evade income or value added taxes;
   - the company indicates in the financial statements simulated items supported by false documents, in order to be able to indicate in the declaration fictitious liabilities or assets lower than the real ones;
   - the company conceals accounting documents, thus hindering the reconstruction of income by the bodies of the Tax Administration.
3. Finance:
   - fraudulent declaration through the use of invoices or other documents for non-existent transactions provided for by Art. 2 Law Decree 10/03/2000 no. 74.

Organizational system control tools
This special part provides for the express obligation to:
- behave in line with the principles expressed in the Code of Ethics and in this Organisational Model;
- comply with the procedures adopted with particular reference to those relating to the management of the sensitive activities indicated above;
- ensure the smooth functioning of cash flows and accounting;
- to ensure the transparency and correctness of accounting documents and related financial flows;
- ensure a correct and transparent process for the management of extraordinary transactions, including the sale of any company assets;
- ensure the veracity of the data prepared and guarantee the correct and precise keeping and custody of accounting and tax records;
- ensure the transparent management of the supply of goods and services;
- comply with tax-tax legislation.

The general control standards to be considered and applied with reference to the Sensitive Activities identified are the following:
- Existence of Formalized Procedures/Guidelines: provisions suitable for providing at least general reference principles for the regulation of sensitive activities;
- Traceability: traceability and ex post verifiability of operations through adequate documentary/IT supports;
- Segregation of tasks: application of the principle of separation of activities between those who authorize, those who execute and those who control;
- Existence of a system of delegations consistent with the organizational responsibilities assigned: there must be formalized rules for the exercise of powers of signature and internal authorization powers.

Criminal Offences under Article 25-*vicies* of Legislative Decree 231/2001
Offences Committed Through Artificial Intelligence Systems

Regulatory references:
- Failure to adopt security measures for artificial intelligence systems and illicit alteration of such systems (Art. 437-bis of the Criminal Code – introduced by Legislative Decree no. 160 of September 9, 2026);
- Illicit dissemination of content generated or altered using artificial intelligence systems (Art. 612-quater of the Criminal Code – introduced by Law no. 132/2025).

Following the introduction of Article 25-vicies of Legislative Decree 231/2001 concerning offences committed through the use of Artificial Intelligence (AI) systems, the Company has identified the following sensitive activities in which the use of AI systems could give rise to the risk of commission of predicate offences.

Sensitive Areas

1. Engineering and Design

Activities relating to:
- use of AI systems for the design of plants, boilers, HRSGs and critical components;
- process simulations;
- automated generation of technical documentation;
- preparation of risk analyses.

231 Risks:
- alteration or manipulation of AI systems;
- use of unvalidated technical data;
- lack of human supervision over outputs affecting safety-critical decisions.

2. Industrial Safety and Process Safety

Activities relating to:
- predictive maintenance systems;
- monitoring of plants and equipment;
- automated control and alarm systems;
- AI-supported HSE assessments.

231 Risks:
- failure to implement adequate safeguards for high-risk AI systems;
- exclusive reliance on algorithmic decisions without human verification.

3. Information Technology and Cybersecurity

Activities relating to:
- development, configuration and management of AI tools;
- use of generative AI systems;
- management of cloud infrastructures;
- administration of AI models and datasets.

231 Risks:
- unlawful alteration of AI systems;
- unauthorized access;
- insufficient traceability of activities performed;
- use of unauthorized AI systems (shadow AI).

4. Procurement and Supplier Management

Activities relating to:
- procurement of AI software and applications;
- selection of technology providers;
- use of external AI platforms and services.

231 Risks:
- acquisition of non-compliant AI systems;
- failure to verify security, reliability and regulatory compliance requirements.

5. Human Resources

Activities relating to:
- CV screening;
- candidate assessment and selection;
- AI-based performance management systems;
- AI-assisted training activities.

231 Risks:
- improper processing of personal data;
- uncontrolled automated decision-making processes.

6. Marketing, Communications and External Relations

Activities relating to:

- automated content generation;
- use of artificially generated images, audio and video;
- website and social media publications.

231 Risks:

- dissemination of falsified content (deepfakes);
- misleading communications or communications infringing third-party rights.

General Control Principles of the Organizational System

The Sofinter Group has adopted the Corporate Policy for the Responsible Use of Artificial Intelligence.

The Sofinter Group recognizes the strategic role of Artificial Intelligence (AI) as a key enabler for innovation in industrial processes, operational efficiency, and the enhancement of the Group's competitiveness, particularly in the areas of engineering, plant management and decision-support activities.

The adoption of AI solutions is guided by a dual objective: on the one hand, to leverage the opportunities offered by advanced technologies to improve the quality, safety and efficiency of the services provided; on the other hand, to ensure that their use remains human-centric, trustworthy and subject to effective oversight, while safeguarding high standards of security and the fundamental rights of all individuals involved.

The Corporate Policy for the Responsible Use of Artificial Intelligence forms an integral part of the Company's governance framework and is coordinated with the principal regulatory and control systems already adopted by the Group, including:

- the Organizational, Management and Control Model pursuant to Legislative Decree 231/2001;
- the Group Code of Ethics;
- the personal data protection management system compliant with Regulation (EU) 2016/679 (GDPR);
- the cybersecurity security and resilience measures implemented in accordance with Directive (EU) 2022/2555 (NIS2).

Within this framework, the Policy establishes a comprehensive, binding and continuously updated governance structure for managing the entire lifecycle of AI systems, from assessment and procurement through deployment, operation and ongoing monitoring.

The framework adopted by the Sofinter Group is based on the principles and requirements set out in Regulation (EU) 2024/1689 (AI Act), which serves as the primary regulatory reference for ensuring the development, deployment and use of safe, transparent and trustworthy AI systems within the European Union.

The adoption of Artificial Intelligence systems by the Sofinter Group is not intended to reduce or limit the safeguards established by labour legislation, the applicable collective bargaining agreement, or any collective agreements in force.

The use of AI must always comply with the principles of human dignity, non-discrimination, fairness, transparency and the protection of employees' rights.