

MICROMED S.R.L.

Organization, Management and Control
Model pursuant to Legislative Decree June 8,
2001.

n. 231

Adopted by determination of the A.U. on

GENERAL INDEX

1 PRESENTATION	6
1.1 COMPANY DATA.	6
1.2 ACTIVITIES CARRIED OUT	6
1.3 INTRODUCTION	6
1.4 ADDRESSEES OF THE GENERAL PART	7
1.5 THE REGULATORY FRAMEWORK	8
1.5.1 THE ADMINISTRATIVE RESPONSIBILITY REGIME	8
1.5.2 ADOPTION OF THE MODEL AS AN EXEMPTION	14
1.5.3 THE COMPANY'S ADOPTION OF THE MODEL	15
1.5.3.1 Rationale for adopting the model	15
1.5.3.2 Goals and objectives of the model	16
1.5.3.3 Preparation of the model	17
1.5.3.4 Model structures and building blocks	18
1.5.3.5 Map of "sensitive" business activities	20
1.5.3.6 Adoption and application of the model	22
1.6 THE SUPERVISORY BOARD	22
1.6.1 ESTABLISHMENT OF THE SUPERVISORY BOARD	22
1.6.2 FUNCTIONS AND POWERS OF THE SUPERVISORY BOARD	23
1.6.3 RELATIONAL ACTIVITIES OF THE SUPERVISORY BOARD	25
1.6.4 INFORMATION FLOWS TO THE SUPERVISORY BOARD	26
1.7 TRAINING AND DISSEMINATION OF THE MODEL	27
1.7.1 STAFF TRAINING	27
1.7.2 INFORMATION TO COLLABORATORS, CONSULTANTS AND OTHERS	28
1.8 THE DISCIPLINARY AND SANCTIONS SYSTEM	28
1.8.1 GENERAL PRINCIPLES	28
1.8.2 GENERAL CRITERIA FOR THE IMPOSITION OF PENALTIES	29
1.8.3 SUBJECTS SUBJECTED	30
1.8.4 MEASURES FOR NON-COMPLIANCE BY EMPLOYEES	31
1.8.4.1 Violations	31
1.8.4.2 Penalties	32
1.8.4.3 Measures for non-compliance by managers	33
1.8.4.4 Violations	33
1.8.4.5 Sanctions	34
1.8.5 MEASURES FOR NON-COMPLIANCE BY DIRECTORS	35
1.8.5.1 Violations	35
1.8.5.2 Penalties	36
1.8.6 SANCTIONS AGAINST COLLABORATORS, CONSULTANTS AND OTHER THIRD PARTIES	36
1.9 APPROVAL, AMENDMENT AND IMPLEMENTATION OF THE MODEL.	37
1.9.1 APPROVAL ADOPTION OF THE MODEL	37

1.9.2	CHANGES AND ADDITIONS TO THE MODEL	37
1.9.3	IMPLEMENTATION OF THE MODEL	38
1.10	APPENDIX	38
1.10.1	DOCUMENTS THAT IMPLEMENT THE PROTOCOLS DEFINED FOR MODEL 231	38
2 STRUCTURE OF SPECIAL PARTS A - B		3G
2.1	SYSTEMATIC BACKGROUND	3G
2.2	THE STRUCTURE OF SPECIAL PARTS A - B	40
2.3	GENERAL PRINCIPLES OF BEHAVIOR IN RISK AREAS	41
2.4	OFFENCES AGAINST PUBLIC ADMINISTRATION	42
2.5	COMPUTER CRIMES AND UNLAWFUL PROCESSING OF DATA	47
2.6	CRIMES OF ORGANIZED CRIME	4G
2.7	CORPORATE CRIMES (ART. 25-TER, LEGISLATIVE DECREE 231/2001)	50
2.8	CRIMES FOR THE PURPOSE OF TERRORISM OR SUBVERSION OF DEMOCRATIC ORDER	53
2.G	CRIMES AGAINST INDIVIDUAL PERSONALITY	56
2.10	RECEIVING, MONEY LAUNDERING, SELF LAUNDERING.	57
2.11	CRIMES INVOLVING NON-CASH PAYMENT INSTRUMENTS	58
2.12	COPYRIGHT INFRINGEMENT CRIMES	5G
2.13	CRIMES RELATING TO FORGERY OF INSTRUMENTS OR SIGNS OF RECOGNITION	60
2.14	CRIMES AGAINST INDUSTRY AND TRADE	60
2.15	TAX OFFENSES	61
2.16	CRIMES AGAINST CULTURAL HERITAGE	63
3 AREA A - RISK ANALYSIS		64
3.1	RISK OF MANAGING RELATIONSHIPS WITH PUBLIC ADMINISTRATIONS AND REGULATORY AUTHORITIES.	64
3.1.1	CRIMES ABSTRACTLY CONCEIVABLE	64
3.1.2	SENSITIVE ACTIVITIES	64
3.1.3	BUSINESS FACILITIES INVOLVED	64
3.1.4	EXISTING CONTROLS	65
3.2	RISK PROCUREMENT OF GOODS, SERVICES AND CONSULTING SERVICES.	65
3.2.1	CRIMES ABSTRACTLY CONCEIVABLE	65
3.2.2	SENSITIVE ACTIVITIES	66
3.2.3	BUSINESS STRUCTURES INVOLVED	67
3.2.4	EXISTING CONTROLS	67
3.3	RISK COMMERCIAL MANAGEMENT - USE OF PRODUCTS WITH PROTECTED TRADEMARKS OR SIGNS OF INDUSTRIAL PROPERTY - CUSTOMER AND SUPPLIER ACQUISITION	6G
3.3.1	CRIMES ABSTRACTLY CONCEIVABLE	69
3.3.2	SENSITIVE ACTIVITIES	70
3.3.3	BUSINESS STRUCTURES INVOLVED	70
3.3.4	EXISTING CONTROLS	71

3.4 RISK ACCOUNTING AND BUDGETING.	71
3.4.1 CRIMES ABSTRACTLY CONCEIVABLE	71
3.4.2 SENSITIVE ACTIVITIES	72
3.4.3 BUSINESS FACILITIES INVOLVED	72
3.4.4 EXISTING CONTROLS	73
3.5 RISK FINANCE AND TREASURY.	74
3.5.1 CRIMES ABSTRACTLY CONCEIVABLE	74
3.5.2 SENSITIVE ACTIVITIES	75
3.5.3 BUSINESS FACILITIES INVOLVED	75
3.5.4 EXISTING CONTROLS	75
3.6 RISK SELECTION, RECRUITMENT, EVALUATION, EMPLOYMENT, REMUNERATION AND INCENTIVE OF THE STAFF	77
3.6.1 CRIMES ABSTRACTLY CONCEIVABLE	77
3.6.2 SENSITIVE ACTIVITIES	78
3.6.3 BUSINESS FACILITIES INVOLVED	78
3.6.4 EXISTING CONTROLS	78
3.7 RISK ADMINISTRATIVE MANAGEMENT OF PERSONNEL.	80
3.7.1 CRIMES ABSTRACTLY CONCEIVABLE	80
3.7.2 SENSITIVE ACTIVITIES	81
3.7.3 BUSINESS FACILITIES INVOLVED	81
3.7.4 EXISTING CONTROLS	81
3.8 RISK MANAGEMENT OF INFORMATION SYSTEMS.	83
3.8.1 CRIMES ABSTRACTLY CONCEIVABLE	83
3.8.2 SENSITIVE ACTIVITIES	84
3.8.3 BUSINESS FACILITIES INVOLVED	85
3.8.4 EXISTING CONTROLS	85
3.G RISK MANAGEMENT CONTROL	88
3.9.1 CRIMES ABSTRACTLY CONCEIVABLE	88
3.9.2 SENSITIVE ACTIVITIES	88
3.9.3 BUSINESS FACILITIES INVOLVED	89
3.9.4 EXISTING CONTROLS	89
3.10 RISK PROPERTY MANAGEMENT AND EVENTS.	8G
3.10.1 CRIMES ABSTRACTLY CONCEIVABLE	89
3.10.2 SENSITIVE ACTIVITIES	90
3.10.3 BUSINESS FACILITIES INVOLVED	90
3.10.4 EXISTING CONTROLS	91
3.11 RISK EVENT AND SPONSORSHIP MANAGEMENT.	G2
3.11.1 CRIMES ABSTRACTLY CONCEIVABLE	92
3.11.2 SENSITIVE ACTIVITIES	93
3.11.3 BUSINESS FACILITIES INVOLVED	93
3.11.4 EXISTING CONTROLS	93
3.12 RISK MANAGEMENT OF CORPORATE COMPLIANCE.	G5
3.12.1 CRIMES ABSTRACTLY CONCEIVABLE	95

3.12.2 SENSITIVE ACTIVITIES	95
3.12.3 BUSINESS FACILITIES INVOLVED	95
3.12.4 EXISTING CONTROLS	96
3.13 RISK MANAGEMENT OF TAX COMPLIANCE.	G7
3.13.1 CRIMES ABSTRACTLY CONCEIVABLE	97
3.13.2 SENSITIVE ACTIVITIES	98
3.13.3 BUSINESS FACILITIES INVOLVED	98
3.13.4 EXISTING CONTROLS	98
3.14 RISK CULTURAL PROPERTY MANAGEMENT.	GG
3.14.1 CRIMES ABSTRACTLY CONCEIVABLE	99
3.14.2 SENSITIVE ACTIVITIES	100
3.14.3 BUSINESS FACILITIES INVOLVED	100
3.14.4 EXISTING CONTROLS	100
4 AREA B - ENVIRONMENTAL AND SAFETY RISK ANALYSIS	102
4.1 MANAGEMENT RISK OF ENVIRONMENTAL ISSUES	102
4.1.1 CRIMES ABSTRACTLY CONCEIVABLE	103
4.1.2 SENSITIVE ACTIVITIES	103
4.1.3 BUSINESS FACILITIES INVOLVED	103
4.1.4 EXISTING CONTROLS	103
4.2 RISK OCCUPATIONAL HEALTH AND SAFETY PROTECTION	105
4.2.1 CRIMES ABSTRACTLY CONCEIVABLE	105
4.2.2 SENSITIVE ACTIVITIES	105
4.2.3 BUSINESS FACILITIES INVOLVED	105
4.2.4 EXISTING CONTROLS	106
5 ANNEXES TO ORGANIZATIONAL MODEL 231	107

1 PRESENTATION

1.1 COMPANY DATA.

Name: Micromed S.r.L.

Registered office: Via Val Padana 126 00141 Rome

Headquarters: Via G. Oberdan 21 00013 Fonte Nuova (RM) P.IVA

01756571004

1.2 ACTIVITIES CARRIED OUT

The company is engaged in the production of medical devices for ophthalmic surgery.

Micromed is a company that has been in the vitreoretinal surgery business for the longest time, in Italy and around the world. It is on its third quality certification in the past 15 years and was the first company to design and manufacture automated pneumatic systems for infusion of viscous and viscoelastic substances, and medical devices consisting of disposable endotamponant gases in canisters either pure or mixed.

1.3 INTRODUCTION

This model was created in implementation of Legislative Decree 231/2001, which establishes, in accordance with certain international conventions, administrative liability for entities for certain crimes committed in their interest or to their advantage.

Pursuant to the implementation of the delegation of authority under Article 11 of Law No. 300 of September 29, 2000, Legislative Decree No. 231 (hereinafter referred to as the "Decree") was issued on June 8, 2001, and entered into force on July 4, 2001, by which the Legislature adapted domestic regulations to international conventions on the liability of legal persons, to which Italy had long been a party. Specifically, these are the Brussels Convention of July 26, 1995, on the Protection of the Financial Interests of the European Communities, the Convention signed in Brussels on May 26, 1997, on Combating Bribery Involving Officials of the European Community or Member States, and the OECD Convention of December 17, 1997, on Combating Bribery of Foreign Public Officials in International and Economic Transactions.

The Decree, on "Discipline of the administrative liability of legal persons, companies and associations, including those without legal personality," introduced into the Italian legal system a regime of administrative liability for the

Entities (to be understood as, associations, consortia, etc., hereinafter referred to as "Entities") for crimes peremptorily listed and committed in their interest or benefit:

- by individuals who hold positions of representation, administration or management of the Entities themselves or of one of their organizational units with financial and functional autonomy, as well as by individuals who exercise, even de facto, the management and control of the Entities themselves, or
- by natural persons subject to the direction or supervision of one of the above-mentioned persons. The liability of the Entity is in addition to the liability (criminal and civil) of the natural person, who materially committed the crime.

The provision of administrative liability under the Decree involves, in the suppression of the criminal offenses expressly provided for therein, Entities that have benefited from the commission of the crime. Among the sanctions that can be imposed, those that are certainly the most onerous for the Entity are represented by interdictory measures, such as the suspension or revocation of licenses and concessions, the prohibition of contracting with the public administration, the disqualification from conducting business, the exclusion or revocation of loans and contributions, and the prohibition of advertising goods and services. The aforementioned liability also arises in relation to crimes committed abroad, provided that the State of the place where they were committed does not proceed for their suppression.

1.4 RECIPIENTS OF THE GENERAL PART

They are the recipients (hereinafter the "Recipients") of this General Part of the Organization, Management and Control Model pursuant to Legislative Decree 231/2001 and are committed to compliance with its contents:

- The director and managers of the Company (so-called top individuals);
- employees of the Company (so-called internal subjects subject to the direction of others).

By virtue of special contractual clauses and limited to the performance of the sensitive activities in which they may participate, the following external parties may be the recipients of specific obligations, instrumental to the adequate performance of the internal control activities provided for in this General Section:

- collaborators, agents and representatives, consultants and, in general, self-employed individuals to the extent that they operate within the areas of sensitive activities;

- suppliers and partners (including in the form of a temporary business association, as well as joint ventures) that operate in a relevant and/or continuous manner within the so-called sensitive areas of activity.

1.5 THE REGULATORY FRAMEWORK

1.5.1 THE ADMINISTRATIVE RESPONSIBILITY REGIME

The system of administrative liability of entities, outlined in Legislative Decree No. 231 of June 8, 2001, is based on the following cornerstones.

First of all, liability arises in connection with the commission of an offense, included among those peremptorily indicated by the legislature, by a natural person who is linked to the entity by a functional relationship, which may be one of representation or subordination, but without the need for identification.

The Decree, in its original draft, listed, among the crimes from the commission of which the administrative liability of Entities is made to derive, exclusively those carried out in relations with the public administration (Art. 25) and, precisely:

- Undue receipt of contributions, financing or other disbursements from the state or other public entity (Article 316-ter of the Criminal Code);
- Fraud to the detriment of the state or other public entity (Article 640, 2nd paragraph, no. 1, Criminal Code);
- Aggravated fraud for obtaining public funds (Article 640-bis of the Criminal Code);
- Computer fraud against the state or other public entity (Article 640-ter of the Criminal Code);
- bribery for an official act (Article 318 of the Criminal Code);
- bribery for an act contrary to official duties (Article 319 of the Criminal Code);
- bribery in judicial acts (Article 319-ter of the Criminal Code);
- Incitement to bribery (Article 322 of the Criminal Code);
- extortion (Article 317 of the Criminal Code);
- Misappropriation to the detriment of the state or other public entity (Article 316-bis of the Criminal Code).

Subsequent to the original structure, Art. 6 of Law No. 409 of November 23, 2001, setting forth "Urgent provisions in view of the introduction of the euro," added the following additional crimes to the list of offenses under the Decree through Art. 25-bis:

- Counterfeiting of money, spending and introduction into the state, with concert, of counterfeit money (Article 453 of the Criminal Code);
- Alteration of coins (Article 454 of the Criminal Code);

- Spending and introduction into the State, without concert, of counterfeit money (Article 455 of the Criminal Code);
- Forgery of revenue stamps, introduction into the state, purchase, possession or putting into circulation of forged revenue stamps (Article 459 of the Criminal Code);
- Counterfeiting watermarked paper in use for the manufacture of public credit cards or stamps (Article 460 of the Criminal Code);
- manufacture or possession of watermarks or instruments intended for the counterfeiting of money, revenue stamps or watermarked paper (Article 461 of the Criminal Code);
- Use of counterfeit or altered stamps (Article 464 of the Criminal Code).

As part of the reform of corporate law, Article 3 of Legislative Decree No. 61 of April 11, 2002, which came into effect on April 16, 2002, introduced the following Article 25-ter into the Decree, which extended the administrative liability of Entities to include the commission of the following corporate crimes under the Civil Code, as amended by the same Decree No. 61/2002.

- false communications (art. 2621 civil code);
- false communications to the detriment of shareholders or creditors (Article 2622 of the Civil Code);
- False statement in prospectus (art. 2623 civil code);
- False statements in the reports or communications of the auditing firm (art. 2624 Civil Code art. repealed);
- impeded control (art. 2625, par. 2, Civil Code);
- Undue return of contributions (Article 2626 of the Civil Code);
- Illegal distribution of profits and reserves (Article 2627 of the Civil Code);
- unlawful transactions in the shares or quotas or of the parent company (Art. 2628 of the Civil Code);
- transactions to the detriment of creditors (Article 2629 of the Civil Code);
- Fictitious capital formation (art. 2632 Civil Code);
- Undue distribution of assets by liquidators (art. 2633 Civil Code);
- Unlawful influence on the General Council (art. 2636 Civil Code);
- agiotage (art. 2637 civil code);
- Obstructing the exercise of the functions of public supervisory authorities (Art. 2638 Civil Code).

L.D. March 2, 2023 No. 19 expanded the reference of corporate crimes beyond those provided for in the Civil Code by inserting the phrase "*or by other special laws*" in paragraph 1.

Laws No. 7 of 2003 and No. 228 of 2003 introduced into the Decree, respectively, Articles 25 quater and 25 quinquies, which extend the administrative liability of Entities to include the commission of crimes for the purpose of terrorism and subversion of the democratic order (Art. 25 quater) and crimes against the individual (Art. 25 quinquies).

These articles were amended by Law No. 7 of January 9, 2006, "Provisions Concerning the Prevention and Prohibition of Female Genital Mutilation Practices," and Law No. 38 of February 6, 2006, "Provisions Concerning the Combating of Sexual Exploitation of Children and Child Pornography including on the Internet," introducing the offenses stipulated in their respective titles.

In addition, Legislative Decree No. 231 of November 21, 2007, implemented Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as Directive 2006/70/EC laying down measures for its implementation (text in force since December 29, 2007), introducing into the list of offenses of Legislative Decree 231/01 also the receiving, laundering and use of money, goods or benefits of illicit origin provided for in Articles 648, 648-bis and 648-ter of the Penal Code.

Law No. 123/2007 also introduced the liability of legal persons for culpable offenses related to homicide or serious and very serious bodily injury in violation of occupational accident prevention regulations, as provided for in Articles 589 and 590 of the Criminal Code. These provisions were reaffirmed by Article 30 of Legislative Decree 81/08 (the so-called "single text" of occupational safety).

On February 27, 2008, the bill introducing Article 24 bis entitled "Computer crimes and unlawful data processing" into Legislative Decree 231/01 was approved. Law No. 90 of June 28, 2024, on "Provisions on strengthening national cybersecurity and computer crimes," inserts into the Criminal Code the new crime of computer extortion, set forth in Art. 629 paragraph 3 of the Criminal Code, which states, *"Whoever, by means of the conduct referred to in Articles c15-ter, c17-quater, c17-sexies, c35-bis, c35-quater and c35-quinquies or by threatening to carry them out, compels someone to do or omit something, procuring for himself or others an unjust profit to the detriment of others, shall be punished by imprisonment from six to 12 years and a fine from 5,000 to 10,000 euros. The punishment shall be imprisonment from eight to twenty-two years and a fine from c,000 euros to 18,000 euros, if any of the circumstances indicated in the third paragraph of Article c28 concur, as well as in the event that the act is committed against a person incapacitated by age or infirmity."* For this new crime, included in paragraph 1-bis of Article 24-bis of Legislative Decree 231/01, there is a fine of 300 to 800 quotas and disqualification penalties of not less than two years (Law No. 90 of June 28, 2024, provided by Article 20, paragraph 1, letter a) the amendment of Art. 24-bis, paragraph 1; by Article 20, paragraph 1, letter b) the introduction of paragraph 1-bis to Article 24-bis; by Article 20, paragraph 1, letter c) the amendment of Article 24-bis, paragraph 2; by Article 20, paragraph 1, letter c) the amendment of Article 24-bis, paragraph 4.

Again, on July 2, 2009, the Senate finally passed bill S.733-B on public safety provisions, which, among other things, provides for the inclusion in the D. Lgs. 231/2001, of Article 24-ter organized crime crimes, namely: crimes of criminal association aimed at reducing or maintaining in slavery, trafficking

of persons, the purchase and sale of slaves and crimes concerning violations of the provisions on illegal immigration as per Art. 12 Legislative Decree 286/1998 (Art. 416, sixth paragraph of the Criminal Code); mafia-type associations, including foreign ones (Art. 416-bis of the Criminal Code); political-mafia electoral exchange (Art. 416 ter of the Criminal Code); kidnapping for the purpose of extortion (Art. 630 c.p.); criminal conspiracy for the purpose of dealing drugs or psychotropic substances (Art. 74 Presidential Decree 309/90), criminal conspiracy (Art. 416, except sixth paragraph, c.p.); crimes concerning the manufacture and trafficking of war weapons, explosives and clandestine weapons (Art. 407 paragraph 2 letter a) c.p.). Finally, Art. 24-ter establishes that if the entity or one of its organizational units is permanently used for the sole or prevalent purpose of enabling or facilitating the commission of the previously indicated crimes, the sanction of permanent disqualification from carrying out the activity applies.

And again on July 9, 2009, the Senate finally approved Bill 1195 B, which, among other things, amends Art. 25 bis of Legislative Decree 231/2001 and inserts in the same Decree Art. 1 - Crimes against industry and trade (Art. 473. - Counterfeiting, alteration or use of trademarks or distinctive signs or of patents, models and designs. Art. 474. - Introduction into the State and trade of products with false signs. Art. 513 - Disturbing freedom of industry or commerce. Art. 515 -Fraud in the exercise of trade. Art. 516 - Sale of foodstuffs not genuine as genuine. Art. 517 - Sale of industrial products with false signs Art. 517-ter - Manufacture of and trade in goods made by usurping industrial property rights. Art. 517-quater. - Counterfeiting of geographical indications or designations of origin of agri-food products. Art. 513-bis -Unlawful competition with threats or violence. Art. 514 -Fraud against national industries) and Art. 25h -offenses related to copyright infringement.

Law 99/2009 inserted Article 25a: Forgery of money, public credit cards, valuables of stamps and in instruments or signs of recognition.

By Law No. 116 of August 3, 2009, the crime of inducement not to make statements or to make false statements to the judicial authority (Art. 377 bis of the Criminal Code) is included in Legislative Decree 23/01.

With Legislative Decree No. 121, of July 7, 2011, under the heading: "Implementation of Directive 2008/99/EC on the protection of the environment through criminal law, as well as Directive 2009/123/EC amending Directive 2005/35/EC on ship-source pollution and the introduction of penalties for infringements," Article 25 undecies on environmental crimes and ship-source pollution was introduced into Legislative Decree 231/01.

Legislative Decree No. 109/2012 (published in Official Gazette No. 172 of July 25, 2012) further expanded the catalog of crimes that can generate direct liability of the entity by including in the

Legislative Decree 231/01 Article 25-duodecies "Employment of third-country nationals whose stay is irregular" "(Article 22, paragraph 12-bis, of Legislative Decree No. 286 of July 25, 1998).

Law No. 190 of Nov. 6, 2012 on provisions for the prevention and suppression of corruption and illegality in the Public Administration was published in Official Gazette No. 265 of Nov. 13, 2012.

Article 1, paragraph 77 of the law reads, "The following amendments are made to Legislative Decree No. 231 of June 8, 2001: a) in Article 25: 1) in the heading, after the word:

"Concussion" the following shall be inserted: ", undue inducement to give or promise benefits"; 2) in paragraph 3, after the words: "319-ter, paragraph 2," the following shall be inserted: "319-quater"; b) in Article 25-ter, paragraph 1, the following shall be added after letter s): "s-bis) for the crime of bribery among private individuals, in the cases provided for in the third paragraph of Article 2635 of the Civil Code, the pecuniary penalty of two hundred to four hundred quotas."

This provision was reformed by Law No. 3 of January 9, 2019, which changed its header ("*Embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office*") and subsequently by Legislative Decree No. 75 of July 14, 2020, which also introduced the offenses under Articles 314 first paragraph, 316 and 323 of the Criminal Code. Most recently, Decree-Law No. 92 of July 4, 2024, converted with amendments into Law No. 112 of August 8, 2024, eliminated Article 323 of the Criminal Code and inserted Article 314 bis of the Criminal Code (Wrongful Destination of Money or Movable Property) and changed the heading again by eliminating the reference to the crime of abuse of office and replacing it with wrongful destination of money or movable property. The same provision, in Article 20, provided for an increase in the penalties for computer crimes under Article 24-bis of Legislative Decree 231/2001, which are now from a minimum of 200 to a maximum of 700 quotas.

Law No. 62/2014 amended Art. 416ter of the Criminal Code, "Political-mafia electoral exchange," Dlgs. No. 39/2014 included the crime of "Solicitation of minors," Article 609undecies of the Criminal Code, and the Legislative Decree

No. 24/2014 amended Articles 600 and 601 of the Criminal Code.

Provisions on the emersion and return of capital held abroad as well as for the strengthening of the fight against tax evasion, introduced the crime of self-laundering. (Article 25 octies Legislative Decree 231/01).

Legislative Decree No. 184 of November 8, 2021 introduced Article 25 *octies*¹, which was subsequently amended by Legislative Decree No. 105 of August 9, 2023, converted with amendments into Law No. 137 of October 9, 2023, about "*Crimes involving non-cash payment instruments and fraudulent transfer of valuables.*"

Law No. 43 of 17/04/2015 concerning urgent measures to counter terrorism amended the crimes of Enlisting for the purpose of terrorism, including international terrorism (Art. 270

quater c.p.) and of Training for Activities with the Purpose of Terrorism, including International Terrorism (Art. 270 quinquies c.p.) as well as Art. 47 of Legislative Decree 231/07 by providing that the FIU shall transmit to the DIA and the Special Currency Police Unit of the Guardia di Finanza, which shall inform the Attorney General's Office, reports of suspicious transactions received by it (and not filed), accompanied by a technical report if they are also related to terrorism as well as to organized crime.

Law No. 68 of May 22, 2015 introduced a new Title VI-bis - Of crimes against the environment - into the Criminal Code, and subsequently Law No. 69 of May 27, 2015 introduced new provisions on crimes against the P.A., mafia association and false accounting.

It has been in force since Nov. 4, 2016, Law 199/2016, which made amendments to Article 603-bis of the Criminal Code (Illegal intermediation and exploitation of labor) by providing for its inclusion among the crimes-prerequisite for the liability of collective entities under Legislative Decree 231/2001.

Legislative Decree No. 38/17 amended bribery among private individuals (Art. 2635 Civil Code) and introduced Art. 2635

bis c.c. (Instigation of bribery among private individuals).

The new Anti-Mafia Code, L. 161/17 amended Art. 25 duodecies by inserting the cases of procuring illegal entry and aiding and abetting illegal immigration referred to in Art. 12 of Legislative Decree 286/98.

The European Law 2017 introduced in DLgs 231/01 art. 25 terdecies "racism and xenophobia" Law Jan. 9, 2019, no. 3 "Measures to combat crimes against the public administration, as well as on the statute of limitations of the crime and on the transparency of political parties and movements," tightened the penalties provided for crimes against the P.A, amended Articles 2635 and 2635-bis of the Civil Code, and introduced trafficking in unlawful influence, Article 346-bis of the Criminal Code, which in turn was amended by the Law in question, into the list of predicate offenses.

On May 16, 2019, Law No. 39/2019 of Ratification and Execution of the Council of Europe Convention on the Manipulation of Sports Competitions was published in the Official Gazette, which introduced Article 25-quaterdecies "Fraud in sports competitions, abusive gaming or betting and gambling exercised by means of prohibited devices" into Legislative Decree 231/01.

Article 1, paragraph 11-bis of Decree Law No. 105 of September 21, 2019, converted with amendments by Law No. 133 of November 18, 2019, amended Article 24-bis of Legislative Decree No. 231/2001 on computer crimes.

Decree Law No. 124/2019, converted with amendments by Law No. 157/2019, introduced the tax offenses provided for in Legislative Decree No. 74 of March 10, 2000, now replaced by Legislative Decree No. 173 of November 5, 2024, effective November 24, 2024, with application of its provisions from 1/1/2026, which established the Consolidated Text of Administrative and Criminal Tax Penalties.

With this rule, the entire national legislation on the repression of violations, tax, administrative and criminal violations in force was gathered into a single body, organizing with new numbering the previously applicable hypotheses, as also recently amended by Legislative Decree No. 87 of June 14, 2024 (Art. 25-quinquiesdecies Dlgs 231/01).

Legislative Decree No. 75 of July 14, 2020 introduced Article 25 sexiesdecies of Legislative Decree 231/01, "Smuggling," while Law No. 22 of March 9, 2022 introduced Articles 25 septesdecies, "Crimes against cultural heritage," and 25 duodevicies, "Laundering of cultural property and devastation and looting of cultural and scenic heritage."

In case of major legislative changes, the organization is required to update its organizational model in order to:

- Supplement the list of predicate offenses in the MOGs by including the newly introduced cases.
- Assess the risks associated with the commission of new crimes and implement appropriate preventive procedures.
- Train staff on new obligations and regulatory changes to ensure proper implementation of internal procedures.

Timely adaptation to regulatory changes is critical to the suitability of the model to be implemented in accordance with Legislative Decree 231/2001.

1.5.2 THE ADOPTION OF THE MODEL AS AN EXEMPTION

The rule provides a specific form of exemption where the company demonstrates that it has put in place a suitable organizational and management model to prevent the commission of crimes (precept) by continuously supervising its operation, effectiveness and updating it as it evolves.

Said models of organization, management and control, must meet the following requirements:

- Identify the activities within the scope of which the crimes under the Decree may be committed;
- Provide specific protocols aimed at planning the formation and implementation of the company's decisions in relation to the crimes to be prevented;
- Identify ways of managing financial resources suitable for preventing the commission of such crimes;
- Provide for information obligations towards the body in charge of supervising the operation of and compliance with the Models;

- Introduce an appropriate disciplinary system to punish non-compliance with the measures specified in the Models.

Where the crime is committed by individuals who hold positions of representation, administration or management of the company or one of its organizational units with financial and functional autonomy, as well as by individuals who exercise, even de facto, management and control over it, the company is not liable if it proves that:

- the management body has adopted and effectively implemented, prior to the commission of the act, suitable organization and management models to prevent crimes of the kind that occurred;
 - a body of the company with autonomous powers of initiative and control has been entrusted with the task of supervising the functioning and observance of the Models and ensuring that they are updated. In small entities, the supervisory tasks referred to in Article 6 c. 1 lett. b) (Supervision) can be carried out directly by the management body;
 - the subjects committed the crime by fraudulently circumventing the Models;
 - there was no failure or insufficient supervision by the supervisory body
- In order to Models.

If, on the other hand, the crime is committed by persons subject to the management or supervision of one of the above-mentioned persons, the company is liable if the commission of the crime was made possible by the failure to comply with the obligations of management and supervision. Said non-compliance is, in any case, excluded if the company, prior to the commission of the crime, adopted and effectively implemented Models suitable for preventing crimes of the kind that occurred, according to an assessment that must necessarily be a priori.

1.5.3 THE ADOPTION OF THE MODEL BY THE COMPANY

1.5.3.1 REASONS FOR ADOPTING THE MODEL

The company has provided for the implementation and adoption of the model to ensure conditions of fairness and transparency in the conduct of the company's business and activities, to protect its position and image, the interests of any shareholders and the work of its employees.

In fact, the company is convinced that the adoption of the Model constitutes not only a valid tool for raising the awareness of all those who work on its behalf, so that they behave correctly and straightforwardly in the performance of their activities, but also an indispensable means of prevention against the risk of commission of crimes and offenses

administrative requirements under the relevant regulations, thus implementing a principle of strict compliance with legality.

To this end, although the adoption of the Model is not provided for by law as mandatory, the company has initiated an analysis project that was carried out in the belief that the adoption and effective implementation of the Model itself not only allow it to benefit from the exemption provided for in Legislative Decree 231/2001, but also improves, within the limits provided by the same, its ability to manage business processes, preventing the risk of committing crimes.

1.5.3.2 GOALS AND OBJECTIVES OF THE MODEL

The purpose of the model is to implement an organic system that prevents the commission of crimes and offenses with the aim of determining in all those who work on behalf of the company the awareness that they may incur criminal and administrative penalties for misconduct.

Specifically, through the adoption of the Model, we aim to pursue the following.

MAIN PURPOSES:

- to determine, in all those who work on behalf of the company in the context of sensitive activities (understood as activities in the context of which the crimes provided for in the Decree may be committed), the awareness that they may incur, in the event of violation of the provisions set forth therein, disciplinary and/or contractual consequences as well as criminal and administrative sanctions that may be imposed on themselves and also on the entity;
- Reiterate that such forms of illegal behavior are strongly condemned, as the same are in any case contrary not only to the provisions of the law, but also to the ethical principles to which the company intends to adhere in the conduct of its business and set forth in the adopted Code of Ethics;
- enable the company, through an action of constant control and careful supervision, monitoring of areas of activity at risk, to intervene promptly to prevent or counteract the commission of the offenses themselves and sanction behavior contrary to its Models.

1.5.3.3 PREPARATION OF THE MODEL

With reference to the issues identified by the legislator in the Decree, the key points developed in the definition of the Model can be briefly summarized as follows:

- Detailed mapping of "sensitive" company activities, i.e., those within the scope of which, by their nature, the crimes referred to in the Decree may be committed and therefore to be subjected to analysis and monitoring;
- analysis of the potential risks for each of them, with regard to the potential ways in which the offenses could be implemented;
- Evaluation of the system of preventive controls to the commission of offenses and, if necessary, definition or adjustment of the planned measures.

For the purpose of preparing the Model, therefore, the following steps were taken:

- to identify the so-called sensitive activities, through prior examination of documentation (organizational charts, proxies, job descriptions, organizational provisions and communications) and a series of interviews with the persons in charge of the various sectors of the entity's operations (i.e., the heads of the various functions). The analysis was prearranged to identify and assess the concrete performance of activities in which unlawful conduct at risk of committing the predicate offenses could occur. At the same time, the control garrisons, including preventive ones, in place and any critical issues for subsequent improvement were assessed;
- to design and implement the actions necessary for the purposes of improving the control system and adapting it to the purposes pursued by the Decree, as well as the fundamental principles of the separation of duties and the definition of authorization powers consistent with the assigned responsibilities;
- To define control protocols in cases where a risk hypothesis was found to exist. Thus, protocols for decision-making and implementation of decisions were defined in this regard.

The principle adopted in the construction of the control system is that the conceptual threshold of acceptability is a prevention system such that it cannot be circumvented except fraudulently.

It then proceeded to carry out a reconnaissance and assessment of the effectiveness of the organization, management and control systems existing and used within the entity and to codify, where necessary in written documents, current company practices aimed at the prevention of illegal conduct identified by Legislative Decree 231/2001.

At the end of a process of codifying the existing organization, management and control practices as well as updating the company's procedures/rules of conduct, the entity has identified the procedures referable to the Model, collected them in special documents kept at the same, bringing them to the attention of the Recipients from time to time and in any case making them available to them also through dissemination in the company's communication channels.

The procedures/rules of conduct traceable to the Model are, of course, integrated with other organizational guidelines, organizational charts, service orders, the system of attribution of powers and company proxies-as functional to the Model-already used or operating within the entity.

1.5.3.4 STRUCTURES AND BUILDING BLOCKS OF THE MODEL

The Model, this "General Part" of which constitutes its descriptive document, is an internal regulatory system aimed at ensuring the formation, implementation and control of the entity's decisions in relation to the risks/offenses to be prevented, consisting of the following "tools."

1. A Code of Ethics and Conduct (setting general guidelines);
2. the "Special Part" of this Model, prepared for the different types of crimes applicable to the entity, which, in view of its particular content, must be susceptible to periodic updates;
3. a system of formalized procedures, aimed at regulating in detail the procedures for making and implementing decisions in the areas at risk of committing the crimes provided for in the Decree, as well as aimed at ensuring the documentation and/or verification of operations in these areas, susceptible to periodic updates;
4. A system of corporate delegation and authority that ensures a clear and transparent representation of the company's decision-making and implementation processes.

As such, the additional key business documents that are references for the model are:

- The Organizational Chart
- The Risk Assessment Document
- The Code of Ethics and Conduct
- The regulations of the Supervisory Board

It should be noted that from the analysis conducted, the possibility of concrete Realization of the crimes of:

- Forgery of money, public credit cards and revenue stamps (Art. 25 bis);
- Crimes for the purpose of terrorism or subversion of domestic and international order (Art. 25c);
- Child exploitation (Art. 25 quinquies.1 lett. a);
- Insider Abuse and Market Manipulation (Art. 25 sexies - L.18.04.05, No. 62);
- failure to disclose conflict of interest (art. 25 ter.1 lett. r) - art. 2629 bis civil code);
- female genital mutilation practices (Article 25c1);
- wiretapping, impediment o interruption unlawful of computer or telematic communications (art. 24 bis - art. 617 quater c.p.);
- Installation of equipment designed to intercept, prevent or interrupt computer or telematic communications (Art. 24 bis - Art. 617 quinquies of the Criminal Code);
- Damage to computer or telematic systems of public utility (Art. 24 bis -Article 635d of the Criminal Code);
- Computer fraud of the person providing electronic signature certification services (Article 24 bis - Article 640 quinquies of the Criminal Code);
- National cybersecurity (Article 24-ter DLgs 231/01, as amended by Article 1, paragraph 11-bis, of Decree Law No. 105 of September 21, 2019, converted with amended by Law No. 133 of November 18, 2019)
- Mafia-type associations, including foreign ones (Art. 24b - Art. 416 bis of the Criminal Code);
- political-mafia electoral exchange (Art. 24 ter - Art. 416 ter of the Criminal Code);
- Kidnapping for extortion (Art. 24b - Art. 630 of the Criminal Code);
- Criminal association for the purpose of dealing drugs or psychotropic substances (Art. 24b - Art. 74 Presidential Decree 309/90);
- Crimes concerning the manufacture and trafficking of weapons of war, explosives and clandestine weapons (Art. 24b - Art. 407 paragraph 2 letter a) c.p.p.);
- forgery of money, public credit cards, and revenue stamps (Art. 25 bis Legislative Decree 231/01);
- Copyright infringement offenses (Art. 25 novies Legislative Decree 231/01)
- Procured unlawful entry and aiding and abetting illegal immigration referred to in Art. 12 of Legislative Decree 286/98 (Art.25 duodecies);
- Racism and xenophobia (Art. 25 terdecies Legislative Decree 231/01);
- Fraud in sports competitions, abusive gaming or betting and gambling exercised by means of prohibited devices (Art. 25 quaterdecies DLgs 231/01);

- Smuggling (Art. 25 sexdecies Legislative Decree 231/01);
- Crimes against cultural heritage (Art. 25 septiesdecies Legislative Decree 231/01);
- Laundering of cultural property and devastation and looting of cultural and scenic property (Article duodevicies Legislative Decree 231/01).

Indeed, these are crimes that, given the organizational structure and activities of the company, do not assume particular relevance because:

- Are substantiated by conduct unrelated to the processes managed by the entity
- planned control garrisons make the possibility of their implementation remote.

1.5.3.5 MAP OF "SENSITIVE" BUSINESS ACTIVITIES

For the above, the main areas and related activities to be analyzed for the purposes set forth in the Decree have been identified based on assessments of the nature of the alleged risks.

The mapping activity, reported in detail in the incipit of the special section, has enabled the identification of the main cases of potential risk/offense and the possible ways in which they could be carried out, within the main company activities identified as "sensitive."

Based on the risk analysis, therefore, two Special Parts were developed:

1. **Special Part A**, structured following the so-called "crime-risk area approach," referring to the types of crimes provided for in the Decree, with the exclusion of crimes resulting from the violation of occupational health and safety (art. 25-septies of Legislative Decree 231/2001) and environmental (art. 25 undecies of Legislative Decree 231/2001) regulations
2. **Special Part B**, structured following the so-called "crime-risk area approach," dedicated only to crimes resulting from the violation of occupational health and safety (Art. 25-septies of Legislative Decree 231/2001) and environmental (Art. 25 undecies of Legislative Decree 231/01) regulations.

This Special Part A, in addition to representing the general principles of conduct by which the activities of Micromed S.r.l. are inspired (with reference to the categories of offenses provided for by Legislative Decree 231/2001 considered abstractly relevant for the Company), identifies, for each area at risk of crime:

- the applicable categories of offenses and the related predicate offenses that can be abstractly perpetrated (for a description of the predicate offenses, please refer to the Appendix "List of 231 Offenses");
- the relevant sensitive activities, i.e., those to the performance of which is connected with the risk of commission of the crimes provided for in the Decree;
- the Structures of Micromed S.r.l. involved in sensitive activities and which, in the abstract, could commit the predicate offences envisaged by the Decree in the interest or to the advantage of the Company, although this identification should not be considered, in any case, exhaustive, given that each corporate subject could, theoretically, be involved by way of complicity. In addition, the competent Units directly reporting to the Structures, as well as company attorneys and top management (Sole Director) are always considered to be included, if they are involved in the areas at risk of crime in accordance with the provisions of the proxy and power of attorney system in force;
- The main preventive controls in place to guard against the risks of the commission of predicate offenses.

In this Special Part A, moreover, so-called "instrumental" risk areas have also been identified, i.e., those areas characterized by particular activities that may take on a supporting (or, precisely, instrumental) character with respect to the commission of certain crimes against the Public Administration (bribery and incitement to bribery), as well as corporate crimes, with precise reference to the cases of bribery among private individuals and incitement to bribery among private individuals.

In addition, across all crime risk areas, the following general control principles were also considered relevant:

- Provision of a system of delegated and proxy powers as well as an organizational system (formalized tasks, roles and responsibilities);
- existence of specific protocols corporate which describe roles, responsibilities, activities, operating methods and controls;
- Segregation of duties between:
 - i. > Who requests / who authorizes and who makes payments for amounts exceeding€ 40,000.00;
 - ii. > Who executes and who controls;
- Ex-post traceability and verifiability of every transaction related to sensitive activities;
- Storage of documentation in order to ensure traceability of the process.

1.5.3.6 ADOPTION AND APPLICATION OF THE MODEL

Adoption of the model is implemented by the administrator, through an appropriate determination.

With the same determination, the director, confers on an ad hoc body to assume the functions of a control body, called the Supervisory Board, with the task of supervising the operation, effectiveness, compliance and updating of the Model itself, as well as ensuring the preparation of suitable operating procedures to ensure its most proper functioning. This SB enjoys freedom of action, independence, autonomy and management power.

1.6 THE SUPERVISORY BODY

1.6.1 ESTABLISHMENT OF THE SUPERVISORY BODY

The exemption from administrative liability, as governed by Art. 6(1)(b).

b) and d) of Legislative Decree No. 231/2001, also provides for the mandatory establishment of a body of the company, endowed with both an autonomous power of control (allowing it to supervise the functioning and observance of the Model) and an autonomous power of initiative, to ensure that it is constantly updated.

The Supervisory Board is appointed directly by the director, it must meet the prescribed requirements of honorability, and it has the necessary knowledge and technical skills to carry out the tasks assigned to it.

The existence and permanence of these subjective requirements are, from time to time, ascertained by the company director both prior to appointment and throughout the period in which he or she remains in office. Failure to meet the aforementioned requirements while in office results in forfeiture of the office.

The Supervisory Board is accountable directly to the director and is not linked to the operating structures by any hierarchical constraints so as to ensure its full autonomy and independence of judgment in carrying out the tasks entrusted to it.

The Body shall regulate the rules for its own operation (should it deem it necessary to expand and better document those already included within this Model) possibly by formalizing them in special regulations or provisions (so-called "Regulations of the Supervisory Body").

For the purpose of carrying out the role and function of the Supervisory Board, the aforementioned body is granted by the director the powers of initiative and control and the prerogatives necessary to carry out the activity of supervising the functioning and compliance of the Models and updating them in accordance with the requirements of the Decree.

In addition, for the specific purposes of carrying out supervisory and control activities, the director, also taking into account the activities of the Supervisory Board, allocates to the same an annual expenditure budget for the performance of the activity that it may use in full managerial autonomy. Said budget will be updated from time to time according to the specific needs that will be determined by the Supervisory Board. Any need to exceed the budget determined by specific requirements will be communicated by the Supervisory Board to the administrator and approved by him/her.

The Supervisory Board, having periodically assessed its adequacy in terms of its organizational structure and conferred powers, proposes to the director any changes and/or additions deemed necessary for its optimal functioning in compliance with current regulations.

The Supervisory Board routinely makes use of the entity's structures to carry out its supervisory and control functions and, where necessary, the support of other corporate functions (such as, for example, the RSPP), or external consultants.

1.6.2 FUNCTIONS AND POWERS OF THE SUPERVISORY BODY

The Oversight and Control Board is given the following powers:

1. Verify compliance with the requirements of the Model by the individuals concerned, reporting any non-compliance and the areas that are most at risk, in view of the violations that have occurred;
2. Verify the efficiency and effectiveness of the Model in preventing the offenses under Leg. 231/2001;
3. Report to the director any need or opportunity to update the Model, where there is a need to adapt it, including in relation to changed business conditions;
4. report to the director, for appropriate action, any ascertained violations of the Model that may result in the entity incurring liability.

For the effective performance of the aforementioned functions, the Supervisory Board is entrusted with the following duties and powers:

- Develop and implement a program of checks on the effective application of corporate control procedures in areas of activity at risk and their effectiveness;
- Periodically check the map of risk areas in order to adjust it to the Changes in activity and/or structure;
- Carry out control activities on the functioning of the model, including through identified internal and/or external functions;
- Conduct targeted audits of situations deemed particularly and risk;
- Verify the adequacy of the information and training initiatives carried out on the principles, values and rules of conduct contained in the Model, as well as the level of knowledge of the same;
- Collect all information regarding any violations of the requirements covered by the model and carry out any subsequent investigations;
- Implement or propose to the governing bodies, according to their respective competencies, the necessary corrective actions to improve the effectiveness of the model;
- Collect, process, and store relevant information regarding the model;
- Monitor the adequacy of the penalty system provided for cases of Violation of the rules defined by the Model;
- coordinating with other company functions, including through special meetings, for the better monitoring of activities in relation to the procedures established by the Model, or for the identification of new areas at risk, as well as, in general, for the evaluation of the various aspects pertaining to the implementation of the Model;
- Promote initiatives to disseminate knowledge and understanding of the principles of the Model and to ensure the preparation of internal organizational documentation necessary for its operation, containing instructions, clarifications or updates;
- Carry out reporting activities to corporate bodies.

To this end, the Supervisory Board will be empowered to:

- Issue regulations and/or provisions intended to regulate the activities of the Supervisory Board itself (should it deem it necessary to specify or, better, detail the provisions contained in this model);
- Access to any and all documents relevant to the performance of the functions assigned to the Supervisory Board under the Decree;

- avail itself, under its direct supervision and responsibility, in agreement with the administrator, of the assistance of persons internal or external to the institution, to whom it delegates the performance of operational verification activities;
- proceed at any time, within the scope of its autonomy and discretion to acts of verification regarding the application of the Model;
- to request and obtain that the heads of company functions and, where necessary, the management body, as well as collaborators, consultants, etc., promptly provide the information, data and/or news requested from them to monitor the various company activities that are relevant under the Model, or to verify its effective implementation by the company's organizational structures;

The work of the Supervisory Board cannot be reviewed by any other body or structure.

The Control and Supervisory Board, as a result of the audits carried out, regulatory changes from time to time as well as the ascertainment of the existence of new areas of activity at risk, highlights to the competent corporate functions the advisability for the entity to proceed with the relevant adjustments and updates to the Model.

The Oversight and Control Board verifies, through follow-up activities, that any recommended corrective actions are taken by the relevant corporate functions.

If there are interpretative issues or questions about the Model, Recipients may Contact the Oversight and Control Board for appropriate clarification.

1.6.3 RELATIONAL ACTIVITIES OF THE SUPERVISORY BODY

The Supervisory Board is responsible to the director for:

- Report periodically on the progress of the model, preparing, at least annually, a written report on the activities carried out, critical issues that have emerged and corrective actions taken or to be taken;
- Promptly communicate, in case of reports received of violations of the Model ex. Legislative Decree 231/2001;

The Oversight and Control Board may be consulted at any time by the director to report on the operation of the Model or specific situations

or, in case of special needs, may inform the corporate bodies directly and on its own initiative.

1.6.4 INFORMATION FLOWS TO THE SUPERVISORY BODY

The Supervisory Board must be constantly informed by management on aspects that may expose the company to risk related to the potential commission of the crimes covered by the Decree.

All employees, managers and all those who cooperate in the pursuit of the purposes of the entity in the context of the various relations they have with it, are required to promptly inform the Supervisory Board about any violation or suspected violation of the Model, its general principles and the Code of Ethics, as well as about their unsuitability, ineffectiveness and any other potentially relevant aspects.

In particular, all of the above parties are required to promptly transmit
To the Supervisory Board the information concerning:

- measures and/or news from judicial police organs, or any other authority, from which it can be inferred that investigative activities are being carried out for the crimes referred to in the Decree, also initiated against unknown persons;
- requests for legal assistance forwarded by managers and/or employees in case of initiation of legal proceedings against them for offenses under the Decree;
- reports prepared by the heads of corporate functions as part of the control activities carried out, from which facts, acts, events or omissions with profiles of criticality with respect to the rules of the Decree may emerge;
- news related to the effective implementation, at all levels of the company, of the Model, highlighting the disciplinary proceedings carried out and any sanctions imposed, or the reasoned measures of dismissal of disciplinary proceedings;
- updating the proxy system;
- any communications from the auditing entity regarding matters that may indicate deficiencies in the Internal Control System, reprehensible facts, observations on the entity's financial statements;
- specific communications on health and safety in the workplace referred to in the relevant Special Part of the Model.

Any information, including from third parties and pertaining to the implementation of the Model itself in areas of activity at risk, must be brought to the attention of the Supervisory Board.

The SB will evaluate the reports received and any consequent measures, at its reasonable discretion and responsibility, hearing, if necessary, the author of the report and/or the person responsible for the alleged violation, and will decide whether to propose to the body competent by law the initiation of disciplinary proceedings against the author of the violation, or whether to dismiss the report. If disciplinary proceedings are initiated, the body holding the action will be required to inform the SB about the developments and outcome of the proceedings.

In any case, the SB, in compliance with the regulations on "whistleblowing" (Legislative Decree 24/2023 and ss.mm.ii.), will act in such a way as to guarantee whistleblowers against any form of retaliation, discrimination or penalization, also ensuring the confidentiality of the identity of the whistleblower, without prejudice to legal obligations and the protection of the rights of the Company or persons wrongly accused and/or in bad faith.

Anyone who violates the aforementioned confidentiality obligations or engages in retaliatory or discriminatory acts against a whistleblower is liable to disciplinary action.

Dismissal, demotion etc. resulting from the reports in this paragraph shall be null and void.

To this end, an e-mail address dedicated to the Supervisory Board is established, to which no one except the aforementioned will have access: odv@micromed.it

Due to the small size of Micromed Srl, as clarified above, while it remains preferable to set up a SB with marked characteristics of third party, competence and extraneousness to Micromed S.r.l., the functions and prerogatives of the SB can be exercised by the A.U., in any case keeping the two functions distinct and autonomous.

1.7 TRAINING AND DISSEMINATION OF THE MODEL

1.7.1 STAFF TRAINING

In order to effectively implement the Model, a specific communication plan has been defined aimed at ensuring wide dissemination to the Recipients of the principles set forth in it as well as the procedures/rules of conduct referable to it. This plan is managed by the competent company functions that coordinate with the Supervisory Board and verify that all Recipients have taken note of this Management and Control Organizational Model.

Training activities are articulated in relation to the roles, functions and responsibilities held by individual Recipients as well as the risk level of the area of activity or process in which they operate.

Training activities are adequately documented, and participation in training meetings is formalized by requesting the signature of attendance. The Supervisory Board monitors that constant updating of training courses is ensured in accordance with changing regulatory and operational requirements and supervises their effective use.

1.7.2 INFORMATION TO COLLABORATORS, CONSULTANTS, AND OTHERS

Persons external to the entity (agents, distributors, suppliers, collaborators, professionals, consultants, etc.) are provided, by the heads of corporate functions having institutional contact with them, with specific information on the policies and procedures adopted by the entity in compliance with the Models and the Code of Ethics. This information also extends to the consequences that conduct contrary to the provisions of the Model or in any case contrary to the Code of Ethics or current regulations may have with regard to contractual relations. Where possible, specific clauses aimed at regulating such consequences are included in the contractual texts.

1.8 THE DISCIPLINARY AND PENALTY SYSTEM

1.8.1 GENERAL PRINCIPLES

The introduction of an adequate system of sanctions, with sanctions proportionate to the seriousness of the violation with respect to the violations of the rules set forth in the Model by the Recipients, is a prerequisite for the full effectiveness of the Model itself.

The rules set forth in the Model are assumed by the Entity in full autonomy, in order to better comply with the regulatory precept that is incumbent on the company itself; therefore, the application of sanctions is irrespective of both the criminal relevance of the conduct and the initiation of any criminal proceedings by the Judicial Authority, in the event that the conduct to be censured integrates a case of crime, whether or not relevant under the Decree. Therefore, the application of sanctions may take place even if the Recipients have exclusively carried out a violation of the principles enshrined in the Model, which do not materialize a crime or do not determine direct liability of the Entity, configuring such a violation as an injury to the

Principle of loyalty and fairness of the employee and external collaborator towards Micromed S.r.l.

In order to comply with the provisions of Legislative Decree 231/2001, the entity has supplemented, within the prescribed limits, the disciplinary system provided by the CCNL by adapting, updating and coordinating the pre-existing system with the regulatory provisions of the aforementioned Decree 231/2001.

The adequacy of the sanctions system to the requirements of the Decree is constantly monitored by the Supervisory Board, which must be informed about the types of sanctions imposed and the circumstances underlying them.

The investigation of violations, possibly on the report of the Supervisory Board, the management of disciplinary proceedings and the imposition of sanctions remain the responsibility of the Company Functions appointed and delegated for this purpose as provided by the Company Disciplinary and Sanctioning System.

1.8.2 GENERAL CRITERIA FOR THE IMPOSITION OF SANCTIONS

Disciplinary sanctions may be applied in the case of violations resulting from, but not limited to:

- Failure to comply with the principles of behavior contained in the procedures set forth in the Model;
- Failure to comply with company procedures concerning the evidence of the activity carried out with regard to the manner of documentation, storage and control of the acts related to the procedures of the Model, so as to prevent the transparency and verifiability of the same;
- Violation and/or circumvention of the control system put in place through the removal, destruction or alteration of the documentation provided for in the Model procedures or by preventing the control or access to information and documentation to the persons in charge, including the Supervisory and Control Body;
- Failure to comply with the provisions on signing authority and the proxy system;
- Failure of hierarchical superiors to supervise the behavior of their subordinates regarding the correct and effective application of the principles contained in the procedures set forth in the Model.

In cases of violation of the provisions of the Model, the type and extent of penalties to be impose will be proportionate to the following general criteria:

1. Severity of noncompliance;
2. level of hierarchical and/or technical responsibility of the violator;
3. Subjective element of conduct (distinction between intent and fault);
4. Relevance of the violated obligations;
5. consequences in the hands of the entity;
6. Possible concurrence of other parties in the liability;
7. aggravating or mitigating circumstances with special regard to professionalism, previous job performance, disciplinary record, and the circumstances under which the act was committed.

The severity of the offense will be assessed on the basis of the following circumstances:

- The concrete timeframe and manner of implementation of the offense;
- The presence and intensity of the intentional element;
- The extent of harm or danger as consequences of the infraction for the institution and employees;
- The predictability of consequences;
- The circumstances under which the infringement took place.

The degree of culpability and recidivism of the offense is an aggravating factor and results in the application of a more severe penalty.

Where more than one offense, punishable by different penalties, has been committed by a single act, the most serious penalty may be applied.

Any imposition of the disciplinary sanction, regardless of the institution of the proceedings and/or the outcome of the criminal trial, shall be guided by the principles of timeliness, immediacy and fairness.

1.8.3 SUBJECTS

Subjects subject to the disciplinary system set forth in this Descriptive Document of the Model, with the peculiarities peculiar to the nature of the working or contractual relationship, are employees, the director and collaborators, as well as all those who have contractual relationships with the entity, within the scope of those relationships.

With particular reference to the persons in charge of carrying out activities related to occupational health and safety, disciplinary sanctions are available to all persons who have specific responsibilities defined by current occupational health and safety regulations as well as the Model.

1.8.4 MEASURES FOR NON-COMPLIANCE BY EMPLOYEES

As far as employees are concerned, conduct by them in violation of the behavioral rules provided for in the Model is considered a breach of the primary obligations of the employment relationship and, therefore, also has relevance as disciplinary offenses, in compliance with the specialized regulations (in particular, applicable CCNL and Supplementary Agreements) and current industry procedures (Article 7 of the Workers' Statute).

1.8.4.1 VIOLATIONS

Pursuant to the combined provisions of Articles 5(b) and 7 of Legislative Decree 231/2001, the stipulated sanctions may be applied against a person who commits disciplinary offenses arising from:

- non-compliance with the principles of conduct and Procedures issued under the same Legislative Decree;
- Lack of and untrue evidence of the activity carried out with regard to the manner of documentation, preservation and control of the documents related to the Procedures, so as to prevent the transparency and verifiability of the same;
- failure of hierarchical superiors to supervise the behavior of their subordinates in order to verify the correct and effective application of the provisions of the Model;
- Failure to train and/or update and/or notify personnel operating in the risk areas of the processes covered by the Model;
- Violation and/or circumvention of the control system, carried out through the removal, destruction or alteration of the documentation provided for in the Procedures or by preventing the control or access to information and documentation to the persons in charge, including the Supervisory and Control Body.

The list of cases is by way of example and not exhaustive.

1.8.4.2 SANCTIONS

The penalties that can be imposed for non-compliance with the rules of the Model are in order of severity:

1. the verbal reprimand;
2. the written reprimand;
3. The fine not exceeding three hours;
4. The suspension from service and pay up to a maximum of 10 days;
5. dismissal with notice;
6. dismissal without notice.

1. The measure of verbal reprimand is applied in cases of minor culpable noncompliance with the principles and rules of conduct stipulated in the Model or procedural errors due to negligence.
2. The measure of written reprimand shall be applied in case of recidivism in the violations referred to in lett. a), or one adopts, in the performance of activities in areas at risk, behavior that does not comply with the requirements of the Model.
3. The measure of a fine is applied if, having already incurred the measure of a written reprimand, one persists in violating the internal procedures laid down in the Model or continues to adopt, in the performance of activities in areas at risk, behavior that does not comply with the requirements of the Model.
4. The measure of suspension from service and salary up to a maximum of 10 days is applied in the case of serious violations of the principles and/or procedures of the Model, such as to cause damage to the entity and expose it to liability to third parties, as well as in cases of recidivism in the commission of offenses from which the application of a fine may result.
5. The measure of dismissal with notice applies in case of adoption, in the performance of activities, of a behavior characterized by significant non-compliance with the requirements and/or procedures and/or internal rules established by the Model, even if it is not likely to configure one of the crimes sanctioned by the Decree.
6. The measure of dismissal without notice shall be applied in the event of the adoption, in the performance of activities, of a conscious behavior contrary to the prescriptions and/or procedures and/or internal rules of the Model, which, although not likely to constitute one of the offenses sanctioned by the Decree, harms the element of trust that characterizes the employment relationship or is so serious as not to

Allow its continuation, even temporarily. Violations subject to the aforementioned sanction include but are not limited to the following intentional conduct:

- a) Violation of the principles and procedures having external relevance and/or fraudulent circumvention thereof, carried out by conduct directed at the commission of an offense relevant under the Legislative Decree;
- b) Violation and/or circumvention of the control system, implemented through the removal the destruction or alteration of the documentation required by the Model or the procedures for its implementation or in the impediment, to the persons in charge and the Supervisory Board, to control and access to the required information and documentation.

1.8.4.3

MEASURES FOR NON-COMPLIANCE BY MANAGERS

With regard to executives, in view of the special fiduciary relationship with the employer, in the event of violation of the general principles of the Model, the rules of conduct imposed by company procedures, including on the report of the Supervisory Board, the director will take against those responsible the measures deemed appropriate depending on the violations committed, taking into account that the same constitute a breach of the obligations arising from the employment relationship.

The disciplinary measures that can be imposed are those provided for in the applicable CCNL disciplinary apparatus and will be adopted in compliance with the procedures provided for in Article 7 of Law No. 300 of May 20, 1970 (Workers' Statute) and the criteria of proportionality and taking into account the seriousness, intentionality and possible recidivism.

1.8.4.4

VIOLATIONS

Violations consisting of:

- non-compliance with the principles of behavior and/or procedures issued under the Model and/or internal rules established by the Model;
- Lack of and untrue evidence of the activity carried out with regard to the manner of documentation, preservation and control of documents related to the protocols, so as to prevent the transparency and verifiability of the same;

- Violation and/or circumvention of the control system, carried out through the removal, destruction or alteration of the documentation provided for in the protocols or by preventing control or access to information and documentation to the persons in charge of control, including the Supervisory Board
- Failure to comply with the provisions on signing authority and the system of delegation of authority, except in cases of extreme necessity and urgency, of which the hierarchical superior shall be promptly informed;
- Failure of hierarchical superiors to supervise, control and monitor their subordinates and about the correct and effective application of the principles of conduct and/or procedures issued under the Model and/or the internal rules established by the Model;
- Failure to comply with the obligation to inform the Supervisory Board and/or the immediate supervisor about any violations of the Model carried out by other employees, of which there is direct and certain evidence;
- Failure to train and/or update and/or communicate to personnel operating within the scope of processes governed by procedures.

The list of cases is by way of example and not exhaustive.

1.8.4.5 SANCTIONS

Due to the special fiduciary nature of the working relationship, which binds those who hold an executive position in the institution, the following sanctions will be applied against those responsible:

1. written blame;
2. dismissal with notice;
3. Dismissal without notice.
4. The measure of written reprimand may be imposed in the case of non-serious violation of one or more behavioral or procedural rules provided for in the Model. Where executives have power of attorney with external power of representation, the imposition of the sanction of written reprimand may also result in the revocation of the power of attorney.
5. The measure of dismissal with notice may be imposed in the event of a serious violation of one or more of the Model's requirements such as to constitute a significant breach.

6. The measure of dismissal without notice may be imposed if the violation of one or more requirements of the Model is so serious as to irreparably damage the relationship of trust such that even temporary continuation of the employment relationship is not possible, such as but not limited to:
- the violation of the principles of behavior and/or procedures issued under the Model and/or internal rules established by the Model having external relevance and/or fraudulent circumvention of the same carried out with a behavior directed to the commission of an offense relevant under the Legislative Decree;
 - the violation and/or circumvention of the control system, put in place through the removal, destruction or alteration of the documentation required by procedures or in the impediment, to the persons in charge and the Supervisory Board, to control and access to the required information and documentation.

1.8.5 PROVISIONS FOR INOSSERVANCE FROM PART OF DIRECTORS

1.8.5.1 VIOLATIONS

Feasible violations by the administrator may include, but are not limited to, the following and non-exhaustive, summarized below:

- non-compliance with the principles of behavior and/or procedures issued under the Model and/or internal rules established by the Model;
- Violation and/or circumvention of the control system, carried out through the removal, destruction or alteration of the documentation provided for in the protocols or by preventing control or access to information and documentation to the persons in charge of control, including the Supervisory Board;
- Violation of the provisions relating to signatory powers and, in general, the system of proxies, except in cases of necessity and urgency, of which the Shareholders' Meeting must be promptly informed;
- Violation of the obligation to inform the Supervisory Board and/or any superordinate person about conduct directed to the commission of an offense included among those included in the Legislative Decree,

1.8.5.2 SANCTIONS

Violation of the rules of this model by the administrator may result in the following to them, based on the criteria listed in Section 6.2 above:

- verbal admonition,
- written warning,
- Fine of € 1,000.00 to €100,000.00,
- suspension from office for a period not exceeding two years,
- removal from office in cases where the violation was so serious as to irreparably undermine the relationship of trust that exists between them and the institution.

The imposition of these sanctions or the dismissal of the relevant proceedings is the responsibility of the Shareholders' Meeting upon the proposal of the Supervisory Board, which is entrusted with the task of initiating and carrying out the relevant investigative activity with consequent proposal whenever the fumus of an infringement occurred emerges.

In case of revocation, the provisions of the Civil Code shall be observed.

Regardless of the application of the protective measure, however, the right to of the entity to bring liability and/or compensatory actions.

1.8.6 SANCTIONS AGAINST EMPLOYEES, CONSULTANTS AND OTHER THIRD PARTIES

With regard to collaborators, suppliers and/or subjects having business relations with the entity, whatever the relationship, even temporary, that binds them to the same, failure to comply with the rules of the Model procedures may, where appropriate, constitute a breach of contractual obligations assumed, with all legal consequences, including with regard to the termination of the contract and/or assignment and may result in compensation for damages suffered by the entity.

To this end, there is provision, especially in the case of "outsourced" activities, for the inclusion in contracts of specific clauses that

- acknowledge the knowledge of the Model adopted pursuant to Legislative Decree 231/01 by third parties,
- require the assumption of a commitment by them to refrain from conduct likely to constitute the offenses referred to in the Model itself (regardless of the actual commission or punishability of the offense),

- regulate the consequences in case of violation of the provisions contained in the aforementioned clause; or, in the absence of such a contractual obligation, a unilateral declaration by the third party or collaborator about the knowledge of the Model and the commitment to base their activities on compliance with its provisions.

1.9 APPROVAL, AMENDMENT AND IMPLEMENTATION OF THE MODEL.

1.9.1 APPROVAL ADOPTION OF THE MODEL

The adoption and effective implementation of the Models constitute, pursuant to Article 6, Paragraph I, lett.

a) of Legislative Decree 231/01, acts of non-delegable competence and emanating from the director. It is therefore the responsibility of the latter to approve and adopt, by appropriate determination, the Model.

This Model was adopted by a determination of the administrator.

1.9.2 AMENDMENTS AND ADDITIONS TO THE MODEL

Subsequent amendments and additions to the reference principles of the Model, aimed at enabling its continued compliance with any subsequent requirements of the Decree, are also left to the non-delegable competence of the director.

Substantive changes include:

- Inclusion of additional Special Parts;
- Changes in some parts of this document;
- Amendment of the regulations of the Supervisory Board;
- Modification of the Penalty System.

It is recognized that the administrator may make any changes or additions of a formal nature to this document, provided that the content remains unchanged in substance, as well as make any changes and additions of similar limited scope in the Special Parts.

1.9.3 IMPLEMENTATION OF THE MODEL

It is the task of the administrator, to provide for the implementation of the Model, through evaluation and approval of the actions necessary for the implementation of its basic elements.

For the identification of such actions, the administrative body is supported by the Supervisory Board.

The director must also ensure, including through the intervention of the Supervisory Board, that the areas of "sensitive" activities and Special Parts of the Model are updated in relation to the need for adjustments that may become necessary in the future.

Finally, the effective and concrete implementation of the adopted Model is ensured:

- By the heads of the various organizational structures (directorates, functions, units organization) of the entity in relation to the risk activities carried out by them;
- by the Supervisory Board, in the exercise of the powers of initiative and control conferred on it over the activities carried out by individual organizational units in "sensitive" areas.

1.10 APPENDIX

1.10.1 DOCUMENTS THAT IMPLEMENT THE PROTOCOLS DEFINED FOR THE 231 MODEL

Following are the documents that form an integral part of the Organization and Control Model pursuant to Legislative Decree 231/01.

- REGULATIONS OF THE SUPERVISORY BODY
- CODE OF ETHICS AND CONDUCT
- ORGANIGRAM
- SPECIAL PART A
- SPECIAL PART B
- RISK ASSESSMENT DOCUMENT

2 STRUCTURE OF SPECIAL PARTS A - B

2.1 SYSTEMATIC PREMISE

In this special part of the Organization, Management and Control Model, it has been deemed necessary to describe and analyze the main cases of offenses provided for by Legislative Decree No. 231/2001, in relation to which, for the type of activity carried out by Micromed S.r.l., there is an appreciable risk of commission within the corporate perimeter.

In particular, the following categories of crimes will be examined: crimes related to relations with the Public Administration, with particular reference to the ordinary relations that Micromed S.r.l. entertains as a commercial entity with the P.A., on the other hand, the risks connected with participation in tenders for services or services offered to the P.A. appearing remote (since the Company does not participate in public evidence procedures as a characteristic feature of its operations), against the Administration of Justice, computer crimes and unlawful data processing, crimes of an associative nature, crimes of a corporate nature and tax crimes, provided for in Articles 24, 24 bis, 24 ter, 25, 25 ter, 25 decies and 25 quinquiesdecies of Legislative Decree 231/2001; the cases of crimes in the exercise of commercial activities provided for in Articles 25 bis, paragraph 1 lett. f) and 25 bis1 will also be examined; the criminal cases provided for in Art. 25 septies, dealing with the crimes of manslaughter and serious and very serious culpable injuries committed in violation of the rules on accident prevention and the protection of hygiene and health at work, the crimes of receiving stolen goods, money laundering, and self-laundering referred to in Art. 25 octies, the crimes concerning non-cash payment instruments referred to in Art. 25 octies 1 and certain environmental crimes provided for in Art. 25 undecies and 25 sexesdecies for which a possible risk of commission is evident for the company's activity, even if remote.

In relation to other types of offenses, not specifically addressed in the following examination, although provided for as predicate offenses by Legislative Decree No. 231/2001 (e.g., counterfeiting of currency, crimes against the individual, sports fraud and others) estimating a practically nonexistent risk of commission based on the type of activity carried out by Micromed S.r.l. and its corporate purpose (formal and substantive), will be excluded in the following listing, in order to make the model, already articulated and in-depth, adhere to the business reality.

In any case, the list of offenses provided for in Legislative Decree 231/01 is attached since the possible commission of an offense with low probability of risk, as a violation of the rules contained in the Code of Ethics, equally entails the adoption of the sanctions provided for in this Model.

2.2 THE STRUCTURE OF SPECIAL PARTS A - B

Micromed S.r.l., in order to facilitate reading, understanding and usability by the Recipients of Model 231, has adopted an amalgamated representation of the "Special Parts."

Therefore, the current structure of the Model includes only two Special Parts in addition to the General Part:

1. Special Part A, structured following the so-called "crime risk area approach."
2. Special Part B, on the other hand, dedicated only to crimes resulting from the violation of occupational health and safety regulations (Article 25-septies of Legislative Decree 231/2001) and environmental crimes (Article 25-undecies of Legislative Decree 231/2001).

This Special Part A, in addition to representing the general principles of conduct by which the activities of Micromed S.r.l. are inspired (with reference to the categories of offenses provided for by Legislative Decree 231/2001 considered abstractly relevant for the Company), identifies, for each area at risk of crime:

- the applicable categories of offenses and the related predicate offenses abstractly perpetratable (Refer to the Annex "List of predicate offenses" for a description of predicate offenses);
- the relevant sensitive activities, i.e., those to the performance of which is connected with the risk of commission of the crimes provided for in the Decree;
- the Structures of Micromed S.r.l. involved in sensitive activities and which, in the abstract, could commit the predicate offences envisaged by the Decree in the interest or to the advantage of the Company, although this identification should not be considered, in any case, exhaustive, given that each corporate subject could, theoretically, be involved by way of complicity. In addition, the competent Units reporting directly to the Structures, as well as company attorneys and top management (Sole Director) are always considered to be included, if they are involved in the areas at risk of crime in accordance with the provisions of the proxy and power of attorney system in force;
- The main preventive controls in place to guard against the risks of the commission of predicate offenses.

In this Special Part A, moreover, so-called "instrumental" risk areas have also been identified, i.e., those areas characterized by particular activities that may take on a supporting (or, precisely, instrumental) character with respect to the commission of certain crimes against the Public Administration (bribery and incitement to bribery), as well as corporate crimes, with precise reference to the cases of bribery among private individuals and incitement to bribery among private individuals.

In addition, across all crime risk areas, the following general control principles were also considered relevant:

- Provision of a system of delegated and proxy powers as well as an organizational system (formalized tasks, roles and responsibilities);
- existence of specific protocols corporate which describe roles, responsibilities, activities, operating methods and controls;
- Ex-post traceability and verifiability of every transaction related to sensitive activities;
- Storage of documentation in order to ensure traceability of the process.

2.3 GENERAL PRINCIPLES OF BEHAVIOR IN RISK AREAS

In order to prevent and impede the commission of the predicate offenses considered as relevant in the performance of the sensitive activities underlying the crime-risk areas identified and analyzed below, all Recipients of the Model are required to comply with the following general principles of conduct, without prejudice to what is indicated in the existing company protocols and the Code of Ethics and Conduct:

- To refrain from engaging in or participating in conduct that, taken individually or collectively, may constitute the predicate offenses;
- refrain from engaging in and adopting conduct that, although it does not, in itself, constitute any of the offenses, may potentially become suitable for the commission of such offenses;
- Refrain from engaging in conduct such as to integrate the offenses, even in the form of conspiracy or attempt, or such as to facilitate their commission;
- refrain from engaging in conduct that does not comply with applicable laws, regulations, and company protocols or, in any case, is not in line with the principles expressed in the Model and the Code of Ethics and Conduct.

2.4 CRIMES AGAINST THE PUBLIC ADMINISTRATION

General notions

Public Administration Entities - Public Officials - Persons in Charge of Public Service.

For the purposes of criminal law, a "Public Administration Entity" is commonly considered to be any legal entity that has public interests in its care and carries out legislative, jurisdictional or administrative activities by virtue of public law rules and authoritative acts.

Although there is no definition of Public Administration in the Criminal Code, according to the Ministerial Report to the same Code, Public Administration includes, in relation to the offenses stipulated therein, "all activities of the State and other Public Entities."

In an attempt to formulate a preliminary classification of the legal entities belonging to this category, it is possible to refer, most recently, to Article 1, paragraph 2, of Legislative Decree 1c5/2001 on the subject of the organization of employment in public administrations, which defines all state administrations as public administrations.

It should be noted that not all individuals acting in the sphere of and in relation to the aforementioned Entities are persons in respect of whom (or by whom) the criminal offenses referred to in Legislative Decree 231/2001 are perfected.

Specifically, the figures that assume relevance for this purpose are "public officials," "public service officers," and other individuals specified in Article 322 bis of the Criminal Code.

"Public official" is defined under Article 357 of the Criminal Code as anyone who exercises a public legislative, judicial or administrative function.

A public administrative function is that function governed by rules of public law and authoritative acts and characterized by the formation and manifestation of the will of the Public Administration or by its being carried out by means of authoritative powers (thus coercive or in any case any activity that represents an explication of discretionary public power with respect to a person who is in a non-equal position with respect to the Authority) or certifying (thus any documentation activity to which the system assigns evidentiary effectiveness).

For the purposes of the notion of public official, the relationship of dependence of the person in relation to the state or other public body is not relevant, but only the exercise of a public function is required; in fact, the status of public official can also be extended to private individuals and, therefore, to exponents of corporate entities of a private nature, invested with the performance of public services or public functions, within the limits and in relation to the performance of these functions.

Our legal system has adopted an 'objective' notion of public official, which disregards the legal nature, public or private, of the subject, but is based exclusively on the activity, on the functions exercised in concrete terms; consequently, it is necessary to assess 'from time to time' the individual functions and activities performed, in order to determine whether the subject concerned holds the status of public official and to establish the nature of the actions carried out by the same subject.

These are, for all intents and purposes, individuals who act in the interest of the state or a public administration, forming or manifesting the will of the public administration, even if they are unrelated to the public administration itself.

They are, by way of example, Public Officials:

- *the physician contracted with the health service (Cass. 24.0c.S2, no. 7241);*
- *members of the commission for testing a public work (Cass. 13.0c.Sc, no. c02c);*
- *Those charged with the delivery of court documents.*

Otherwise, they do not hold the title of public official, all those individuals who perform preparatory duties in the formation of the will of the entity (e.g., administrative secretaries).

The term "person in charge of a public service" means, according to Article 358 of the Criminal Code, anyone who, in any capacity, performs a public service, that is, an activity regulated in the same forms as the public function, but characterized by the lack of the powers typical of the latter and excluding the performance of simple orderly tasks and the performance of merely material work.

Regarding the framing of the subject, case law has pointed out a number of 'telltale indices' of the public character of an entity, in relation to which the case history on the subject of joint-stock companies with public participation is emblematic.

In particular, reference is made to the following indices: submission to a control and guidance activity for social purposes, as well as a power of appointment and revocation of directors by the State or other Public Entities; the presence of a convention and/or concession with the Public Administration; financial contribution by the State; the presence of public interest within the economic activity.

In this case, too, the current legal system follows an 'objective' notion, according to which, the discriminating element in indicating whether or not a person holds the status of a 'public service appointee' is the functions entrusted to that person, which must have as their object the care of public interests or the satisfaction of general interests; on the other hand, the legal nature of the entity is not the determining element.

Consequently, even individuals belonging to the same category, may be differently qualified (as public service appointees or not) depending on the activity concretely performed and the sphere in which this activity takes place.

It is therefore necessary to verify, on a case-by-case basis, the correct placement of the subject.

Law 2S.OS.2000 No. 300 extended the qualification of public official and person in charge of a public service to members of the bodies of the European Communities and officials of the European Communities and Foreign States, analytically specified in Article 322 bis of the Criminal Code.

Recent regulatory amendments (Anti-Corruption Law No. 3/2015), have further expanded the group of stakeholders to include, in addition to public officials and those in charge of a public service, "other persons specified in Article 322 bis of the Criminal Code."

The subjects listed in Article 322 bis of the Criminal Code are as follows:

"(1) the members of the Commission of the European Communities, the European Parliament, the Court of Justice and the Court of Auditors of the European Communities;

2) Officials and servants employed under contract under the Staff Regulations of Officials of the European Communities or the Conditions of Employment of Servants of the European Communities;

3) persons seconded by the member states or any public or private entity to the European Communities, who perform functions corresponding to those of officials or agents of the European Communities;

4) members and employees of bodies established on the basis of the Treaties establishing the European Communities;

5) those who, within other member states of the European Union, perform functions or activities corresponding to those of public officials and those in charge of a public service;

(5a) Judges, the Prosecutor, Assistant Prosecutors, officers and agents of the International Criminal Court, persons seconded by the States Parties to the ICC Treaty who exercise functions corresponding to those of officers or agents of the ICC, and members and employees of bodies established on the basis of the ICC Treaty.

5-ter) persons performing functions or activities corresponding to those of public officials and by public service officers within public international organizations;

5-c) members of international parliamentary assemblies or an international or supranational organization and to judges and officials of international courts."

5d) persons performing functions or activities corresponding to those of public officials and public service officers within non-EU states, when the act offends the financial interests of the Union.

In addition, Article 322 bis of the Criminal Code in its second paragraph refers to: "persons performing functions or activities corresponding to those of public officials and public service officers within other foreign states or international public organizations."

The rule then specifies that the persons named are assimilated to public officials, if they perform corresponding functions, and to persons in charge of a public service in other cases.

The recent Legislative Decree 75/2020 establishes that in relation to all crimes against public administration referred to in Article 24, liability is expanded to include cases in which the European Union is harmed.

In relation to crimes against the Public Administration, it is prohibited to:

- to hold relations with the Public Administration, except by those persons delegated to do so in accordance with the organizational system, the system of proxies and powers of attorney and the internal regulatory system;
- Engage in conduct that fosters any situation of conflict of interest, including with respect to the Public Administration;
- Forcing someone, with abuse of his or her position and powers, to give or promise unduly to himself or a third party, money or other benefit;
- grant or pay sums of money or other benefits in favor of Public Officials and/or Persons in Charge of a Public Service, or to persons close to them, belonging to the Public Administration, Public Entities and/or persons assimilated to them of the Italian State, the European Communities and foreign states, except in the case of gifts or utilities of modest value and/or having a symbolic value and/or falling within normal business courtesy;
- To submit to the unlawful request of the Public Official and/or the Person in Charge of a Public Service who, with abuse of his or her quality and powers, induces someone (the person working in Micromed S.r.l.) to unduly give or promise to himself or others close to him or her, money or other benefit;
- Making promises of any kind and species (employment, internship, etc.) or granting advantages of any kind in favor of Public Officials and/or Persons in Charge of a Public Service,

as well as for the benefit of other individuals or legal entities, however traceable to the sphere of interest of the above-mentioned subjects;

- Perform services in favor of third parties generally not directly related to and corresponding to what is contractually agreed upon with such parties;
- grant and pay to assignees of professional assignments sums that are not adequately proportionate to the work performed, even in view of market conditions;
- Make payments to parties other than the contracting party;
- during a business negotiation, request or relationship with the Public Administration, improperly influence the decisions of the counterparty, including those of officials dealing with or making decisions on behalf of the Public Administration and/or indulge in conditioning and pressure aimed at determining decisions that are not in line with the dictates of the Articles of Association, company protocols, the Code of Ethics and Conduct and this Model;
- to be represented, in dealings with the Public Administration, by a consultant or other third party not adequately and formally authorized, and in any case in the event that situations of conflict of interest may arise;
- To provide, draw up or deliver to Public Officials and/or Persons in Charge of a Public Service statements, data or documents in general with inaccurate, erroneous, incomplete, deficient and/or false contents, in order to obtain certifications, permits, authorizations and/or licenses of any kind or species, or to obtain public disbursements, contributions or subsidized financing;
- to provide, draw up, exhibit or deliver to Public Officials and/or Persons in Charge of a Public Service statements, data, information or documents in general having contents that are intentionally artificial, inaccurate, erroneous, incomplete, deficient and/or false, within the scope of any activity of a business nature carried out by the Company;
- make, directly or indirectly (through intermediaries), donations or promises of money or other benefits of any kind to Public Officials and/or Persons in Charge of a Public Service for the purpose of speeding up, facilitating or simply ensuring the performance even of a routine activity or an activity, in any case, lawful and legitimate within the scope of the duties proper to public officials;
- Allocate sums received from the Public Administration by way of disbursements, contributions or financing for purposes other than those for which they were intended;
- making undue promises or giving money or other benefits, of any kind, to an intermediary person (such as a consultant) who has existing or alleged relations with a Public Official/Public Service Officer, as the price of his or her unlawful mediation to the same, in order to pursue an interest of the Company.

This requires:

- Make statements to national or community public bodies for the purpose of obtaining of disbursements, contributions or funding, containing only authentic and accurate elements;
- Adopt behavior characterized by the principles of integrity, honesty, transparency and good faith in connection with any business activity to be undertaken;
- ensure compliance with the principles of fairness, transparency and good faith in any professional relationship that is undertaken with members of the Public Administration or with individuals who qualify as Public Officials or Persons in Charge of a Public Service;
- define in writing any type of agreement with consultants and collaborators in a way that makes the terms of the agreement clear-especially with regard to the type of assignment/transaction and the underlying economic conditions.

2.5 COMPUTER CRIMES AND UNLAWFUL DATA PROCESSING

(Art. 24-bis, Legislative Decree 231/2001)

In relation to computer crimes and unlawful data processing, it is prohibited to:

- Abusively breaking into a computer or information system protected by security measures against the will of the holder of the right of access;
- Accessing the computer or telematic system, or parts thereof, or databases of public or private entities, or parts thereof, by not possessing access credentials or through the use of credentials of other authorized parties;
- destroying, deteriorating, erasing, altering, suppressing information, data or computer programs of others or even merely endangering the integrity and availability of information, data or programs used by the State or other Public Entity or pertaining to it or otherwise of public utility;
- Introduce or transmit data, information or programs for the purpose of destroying, damaging, rendering wholly or partially unserviceable, hindering the operation of public utility computer or telematic systems;
- Alter, through the use of electronic signatures or otherwise in any way, computer documents;
- Produce and transmit documents in electronic format containing false and/or altered data;
- Fraudulently intercepting and/or disseminating, by any means of public information, communications related to a computer or telecommunications system or between multiple systems;

- use unauthorized technical devices or software tools (e.g., viruses, worms, Trojans, spyware, dialers, keyloggers, rootkits) designed to prevent or interrupt communications related to a computer or telecommunications system or between multiple systems;
- Abusively possess, procure, reproduce or disseminate access codes or otherwise Suitable means of accessing a system protected by security measures;
- procuring, reproducing, disseminating, communicating, making available to others equipment, devices or programs for the purpose of unlawfully damaging a system or the data and programs pertaining thereto, or promoting the interruption or alteration of its operation;
- Remove the antivirus software installed on the computer tools provided to users;
- Install additional software/programs than needed for the needs related to business operations;
- Forcing someone to do or omit something by the commission of the conduct described above, or the threat to do it;
- circumvent or attempt to circumvent corporate security systems (e.g., antivirus, firewalls, proxy servers, etc.);
- Leave one's personal computer unattended outside the workplace and without password protection or change/alter the configurations set.

Corporate Structures and, in particular, those in relevant positions in the use and administration of information systems, must base their actions on the following general principles:

- Confidentiality-ensuring that a particular piece of information is preserved from improper access and is used only by authorized individuals. Confidential information must be protected both at the transmission stage and at the storage/storage stage, so that the information is accessible only to those who are authorized to know it;
- integrity-ensuring that any business data is really what was originally entered into the computer system and has been modified only in a legitimate manner. It must be ensured that information is handled in such a way that it cannot be tampered with or changed by unauthorized parties;
- availability-guaranteeing the retrievability of business data according to process continuity needs and in compliance with regulations requiring their historical preservation.

2.6 ORGANIZED CRIME OFFENSES

(Article 24-ter, Legislative Decree 231/2001) and Inducement not to make statements or to make False statements to the judicial authorities (Article 25-decies, Legislative Decree 231/2001)

All those acting on behalf of the Company must comply with the principles of integrity, prudence, fairness, transparency and honesty, observing the following requirements:

- anyone who, acting in the name or on behalf of the Company, comes into contact with third parties with whom the Company intends to enter into business relations or should have relations of any kind with them, must:
 - To inform these parties of the commitments and obligations imposed by the Code of Ethics and Conduct and Model 231 and to demand compliance with them on the basis of express contractual provisions;
 - immediately terminate any relationship with individuals who refuse or otherwise show unwillingness to comply with the Code of Ethics and the Model;
- Periodically verify the correctness, effectiveness, appropriateness and compliance with social interests of the services requested, provided by or for third parties, so as to ensure the establishment and maintenance only of correct business, financial and consulting relationships, truly responsive to social interests and marked by effectiveness, transparency and appropriateness.

In addition, the principles of:

- prudence, accuracy and objectivity in selecting, identifying or otherwise entering into and continuing relationships with third parties and in determining the conditions pertaining to the relationship. Relationships with counterparties may be established only after careful and documented due diligence, verifying, among other things, that there are no circumstances that could lead one to believe that the counterparty is operating illegally in Italy or abroad;
- fairness, transparency and accuracy in accounting entries, tax compliance and the audits that are a prerequisite to it.

In particular, Recipients are expressly prohibited from:

- Use, even occasionally, the Company or one of its Structures/Business Units for the purpose of enabling or facilitating the commission of one or more organized crime offenses;
- Perform services in favor of third parties that are not adequately justified in the context of the contractual relationship established with them;
- Recognize fees in favor of third parties that are not adequately justified in relation to the type of assignment to be performed and current local practices;

- Receive compensation for supplies or services that do not exist or are outside the ordinary business of the Company;
- Providing, directly or indirectly, funds for the benefit of individuals who pursue, directly or as front men, organized crime purposes, facilitating them in the pursuit of their criminal objectives through the provision of financial resources or otherwise increasing their economic availability;
- Use violence or threats against a person called upon to make before the judicial authority statements that can be used in criminal proceedings so that the same person does not make statements or makes false statements;
- Promising to offer money or other benefits to a person called upon to make before the judicial authorities statements that can be used in criminal proceedings so that the same person does not make statements or makes false statements;
- Influencing in any way the willingness to answer of persons called upon to make statements before the judicial authority, determining them to make false statements or inducing them to avail themselves of the right not to answer.

In light of the above, in order to prevent the commission of the crimes in question, the Company adopts standards of conduct marked by:

- verify that any financial transaction presupposes prior knowledge of the beneficiary, at least the direct beneficiary, of the relevant sum of money;
- Verify the commercial and professional reliability of third-party Recipients;
- Verify that the data collected regarding relationships with third parties is complete and up-to-date both for the correct and timely identification of them and for a valid profile assessment;
- Verify the regularity of payments, with reference to the full coincidence between recipients and originators of payments and counterparties actually involved in the transactions, with explicit description of the underlying relationship in the reason for payment.

2.7 CORPORATE CRIMES (ART. 25-TER, LEGISLATIVE DECREE 231/2001)

As a general rule and in order to prevent the commission of corporate crimes, Recipients carrying out their activities within the areas at risk are required to comply with the following general principles of conduct:

- Maintain a conduct marked by the principles of fairness, transparency and cooperation, ensuring full compliance with legal and regulatory provisions, in the performance of all activities aimed at the acquisition, processing, management and communication of data and information, in order to provide members and third parties with

true and fair information about the financial position, results of operations and financial position of the Society.

In this regard, Recipients are prohibited, in particular, from:

- Providing, drafting or transmitting inaccurate, erroneous, incomplete, deficient and/or misrepresented data or documents, such as to configure an incorrect description of the reality, regarding the Company's economic, asset and financial situation;
- Alter or, in any case, report incorrectly, the data and information intended for the preparation and drafting of corporate documents of an asset, economic and financial nature;
- illustrate data and information in such a way as to provide an inaccurate and untrue representation of the Company's financial position, results of operations, and financial position and the development of related activities;
- Strictly observe all the rules set up to protect the integrity and effectiveness of the share capital, in order not to harm the guarantees of creditors and third parties in general. In this regard, Recipients are prohibited, in particular, from:
 - a) return, even simulated, contributions to shareholders or release them from the obligation to make them, outside the cases of legitimate reduction of share capital;
 - b) distribute profits or advances on profits not actually earned or to be allocated by law to reserves, as well as distribute reserves, including those not established with profits, which may not be distributed by law;
 - c) Make reductions in share capital, mergers or demergers, in violation of the provisions of the law, thereby causing damage to creditors;
 - d) Carry out fictitious formation or increase of share capital by allocating shares for less than their par value when increasing share capital;
 - e) purchase or subscribe for shares of the Company outside the cases provided for by law, thereby causing injury to the integrity of the share capital or reserves not distributable by law;
 - f) make available to shareholders and other Corporate Bodies all documentation on the management of the Company necessary to carry out the control activities legally attributed to them. In this regard, Recipients are particularly prohibited from engaging in conduct that materially impedes, or otherwise hinders, the performance of control activities by shareholders and other Control Bodies, through the concealment of documents or the use of other fraudulent means;
 - g) Ensure the smooth operation and performance of the Company and corporate bodies, facilitating and ensuring all forms of internal control

on corporate management required by law, as well as promoting the free formation and decision-making of the Company.

In this regard, for Recipients:

- A) it is forbidden to engage in conduct that materially prevents, or otherwise obstructs, through the concealment of documents or the use of other fraudulent means, the performance of the activity of control or review of corporate management by shareholders; it is forbidden to engage in simulated or fraudulent acts during Shareholders' Meetings aimed at altering the regular procedure for the formation of the will of the Shareholders' Meeting;
- B) is obliged to strictly observe and comply with all legal provisions protecting the integrity and effectiveness of the share capital, in order not to harm the guarantees of creditors and third parties in general;
- C) abide by the precise rules of conduct set forth in the relevant protocols in the conclusion of contracts with other private companies, omitting to give or promise money or other benefits, so as not to induce directors, general managers, managers in charge of drafting accounting documents, liquidators or persons subject to the management or supervision of one of them, to violate the obligations inherent in their office or the obligations of loyalty (please also refer to the general principles of conduct set forth in Section 2.1, to be considered applicable also in the management of relations with private parties);
- D) make timely, correct and good faith reporting to the Supervisory Authorities in all cases required by law or regulations. To this end, Recipients must:
- E) send to the Supervisory Authorities the reports required by law or regulations or otherwise required of the Company in a timely, complete and accurate manner, transmitting for this purpose all the data and documents required or requested;
- F) indicate in the aforementioned reports true, complete and correct data, giving indications of any relevant facts relating to the Company's economic, asset or financial situation;
- G) Avoid any behavior that may hinder the Supervisory Authorities in the exercise of their prerogatives (through, for example, lack of cooperation, obstructive behavior, reticent or incomplete responses, specious delays).

2.8 CRIMES FOR THE PURPOSE OF TERRORISM OR SUBVERSION OF LAW AND ORDER DEMOCRATIC

(Art.25-quater, Legislative Decree 231/2001)

In order to prevent and prevent the occurrence of the crimes in question, Recipients are prohibited from:

1. Engage in conduct that does not comply with the laws and regulations in force in any geographic context and sphere of operation, including the prevention of crimes relating to terrorism and subversion of the democratic order;
2. establish relationships (orders, contracts, consultancies or any commercial and/or financial transaction) with individuals, entities, companies or associations in any form constituted, in Italy or abroad - either directly or through intermediaries - that are known or have reason or suspicion to believe are part of or are in any case linked or have relationships of any nature with criminal associations or groups (e.g. included in the Reference Lists defined by the Bank of Italy, UN, EU, OFAC, etc.), or in any case whose identity, integrity and propriety, as well as, in the case of companies, actual ownership or control ties, have not been ascertained with accuracy, diligence and in a traceable and documented manner;
3. establish relationships with individuals who refuse or show reticence in providing information relevant to their correct, effective and complete knowledge or with respect to whom there are elements of suspicion also due to possible operations in non-cooperative countries, or who request or offer services that, although abstractly advantageous for the Company, present profiles of suspiciousness or irregularity;
4. providing, directly or indirectly, funds in favor of persons who intend to carry out one or more crimes for the purpose of terrorism or subversion of the democratic order, or in favor of persons who pursue, directly or indirectly, the purpose of terrorism or subversion of the democratic order, facilitating them in the pursuit of their criminal objectives through the provision of financial resources or otherwise increasing their economic availability. Relevant for this purpose are funds and economic resources disbursed in favor of a person or group in the knowledge-or at least with reasonable suspicion-that:
 - Pursues purposes of terrorism or subversion of democratic order;
 - the recipient of the funds will allocate them to such individuals or groups;
 - financial resources will be used to commit the crimes in question;
5. collecting, disbursing, or making available goods or money, in any way realized, intended to be used in whole or in part for the performance of conduct with the purpose of terrorism;

6. Misappropriate, destroy, disperse, suppress or deteriorate property or money subject to seizure for the purpose of preventing the financing of conduct for terrorist purposes;
7. Perform services in favor of third parties that are not directly related and corresponding to what is contractually agreed upon with such parties;
8. make payments to numbered or numbered accounts or in cash (except for modest amounts and in compliance with the company's cash management procedure) and in any case to parties other than the contractual counterparty;
9. make payments, as well as disburse donations or other benefits, to entities-individuals or legal entities-that are on the Lists drawn up by international organizations (e.g., UN, EU, OFAC, etc.) in order to prevent the financing of terrorism and money laundering;
10. Recognize fees or commissions in favor of third parties that do not find adequate justification or that are not adequately proportionate to the work performed, including in view of market conditions, the type of assignment to be performed, and current local practices;
11. taking on or assigning orders or carrying out any transaction that may present an anomalous character in terms of type or object, or that may lead to the establishment or maintenance of relationships that present anomalous profiles from the point of view of the reliability of the same and/or the reputation of the counterparties;
12. to use, even occasionally, the Company or one of its corporate functions for the purpose of enabling or facilitating the commission of the offenses referred to in this paragraph;
13. harboring or providing hospitality, means of transportation, means of communication or any other support to persons who participate in subversive associations or associations with terrorist aims.

In addition, there is an obligation to ensure the regularity of the passive cycle in order to ensure that:

- every payment is made by bank transfer (with the only exceptions defined in the company's procedure for cash management), the use of cash or similar payment instruments being prohibited, and in such a way that traceability is guaranteed (amount, name/designation of the recipient, reason for payment and account number);
- the payment is made exclusively to the current account indicated in the contract or in the relevant accounting documentation and in favor of the contractual counterparty, being excluded the possibility of making payments to encrypted accounts, in the name of third parties, in a country outside that of the contracting parties or that of execution of the contract or to entities that are included in the Lists drawn up by international organizations (e.g., UN, EU, OFAC, etc.) in order to prevent the financing of terrorism and money laundering;
- the payment corresponds exactly to the contractually agreed amount;

- there is full coincidence between recipients/payment originators/requests and counterparties actually involved in the transactions;
- Ensure that payments or reimbursements of expenses, fees, discounts, credit notes, or the reduction in any other form of the amount due in favor of internal parties or third parties to the Company occur only if:
 - i. find adequate justification in light of the contractual relationship established with them;
 - ii. represent the consideration of goods, services, services, etc. actually received by the Company;
 - iii. Are supported by justification and properly documented;
- identify the trustworthiness of consultants, suppliers, and, more generally, of third party counterparties (hereinafter, jointly, "counterparties"), in order to verify their honorability and reliability, including from the point of view of the correctness and traceability of economic transactions with them, avoiding the establishment or continuation of relationships with parties that do not present or maintain over time adequate requirements of transparency and fairness;
- Monitor over time whether counterparties continue to meet the requirements of reliability, fairness, professionalism and honorability;
- select counterparties based on criteria of transparency, cost-effectiveness and fairness, ensuring the traceability of activities to prove the aforementioned criteria;
- Carry out a preventive verification activity aimed at ascertaining the reputation, honorability, reliability, professionalism, competence and experience of the counterparties, as well as suitable for identifying any conditions of incompatibility and conflict of interest or the existence of criminal convictions or sanctions against them;
- ascertain the location of the counterparty's registered office or residence, which must not be located in countries with a "privileged tax regime," except in the case of contracts to be entered into with counterparties residing in such countries and such countries are the same as those in which the services covered by the contract will be performed;
- Determine the minimum requirements to be met by the bidding parties and set the criteria for evaluating the bids;
- Identify the organizational unit responsible for contract execution.

2.9 CRIMES AGAINST THE INDIVIDUAL PERSONALITY

(Art. 25-quinquies, Legislative Decree 231/2001) and Employment of third-country nationals whose stay is irregular (Art. 25- duodecies, Legislative Decree 231/2001)

In order to prevent and prevent the occurrence of the crimes in question, Recipients are prohibited from:

- consider any economic condition to take precedence over worker protection and relevant regulations;
- Fail to report deficiencies or irregularities in the documentation received from potential candidates or employees (e.g., residence permit);
- Establish relations of any kind (including labor relations - including by external collaborators, suppliers or business partners) with parties who are known or have reason to suspect that they are using the labor of minors or illegally hired personnel or are otherwise operating in violation of laws and regulations on the protection of workers' rights;
- Using, hiring or employing labor, including through temporary employment companies, subjecting workers to exploitative conditions and taking advantage of their state of need;
- Repeatedly pay workers wages in a manner that is manifestly different from the relevant national or territorial collective bargaining agreements or otherwise disproportionate to the quantity and quality of work performed;
- Repeatedly violate regulations on working hours, rest periods, weekly rest, mandatory leave, vacation, etc;
- Subject workers to degrading working conditions, surveillance methods or housing situations;
- Carry out transportation of foreigners to the territory of the Italian state;
- Engaging in other acts aimed at illegally procuring the entry of foreigners into the territory Of the Italian state or other state.

In addition, there is a requirement to:

- Hiring the Company's staff with regular employment contracts, in accordance with the relevant laws and collective bargaining agreements, including in terms of remuneration (consistency with respect to the quantity and quality of work performance), working hours, rest periods, weekly rest, mandatory leave, vacations, etc;
- Comply with the relevant regulations for hiring non-EU personnel;
- in the event that temporary work is used through special agencies, ensure that such agencies use workers who are in compliance with the regulations on residence permits and do not act in violation of the regulations in

- materia of brokerage unlawful and exploitation of labor, requiring expressly the commitment to compliance with the Model adopted by the Company;
- ensure, with appropriate contractual clauses, that any third parties with whom the Company collaborates (suppliers, consultants, etc.) make use of workers in compliance with the regulations on residence permits and do not act in violation of the regulations on illegal brokering and exploitation of labor, expressly requiring a commitment to comply with the Model adopted by the Company;
 - Monitor staff working conditions periodically, such as through labor climate surveys.

2.10 RECEIVING STOLEN GOODS, MONEY LAUNDERING, SELF-LAUNDERING

and use of money, goods or benefits of illicit origin, as well as self-money laundering (Article 25-octies, Legislative Decree 231/2001)

In order to prevent and prevent the occurrence of the crimes under analysis, it is prohibited to:

- Receive, transmit, transfer, sell, purchase or otherwise move, goods, money or other utilities, in the knowledge or doubt of their illicit origin;
- Violate existing legal regulations about the method of collection and/or payment;
- establish relationships (consultancy or any commercial and/or financial transaction) with subjects, entities, companies or associations in any form established, in Italy or abroad - whether directly or through intermediaries - that are known or have reason or suspicion to believe are part of or are in any case linked or have relationships of any kind with criminal associations or groups (for example, included in the Reference Lists defined by the Bank of Italy, UN, EU, OFAC, etc.), or in any case whose identity, integrity and propriety as well as, in the case of companies, actual ownership or control ties have not been ascertained with accuracy, diligence and in a traceable and documented manner;
- Employing, substituting or transferring in economic, financial, business or speculative activities, money, goods or other utilities originating from a non-negligent crime or carrying out, in relation to them, other transactions so as to hinder the identification of their criminal origin.

It is, likewise, made obligatory to:

- to behave correctly, transparently and cooperatively, in compliance with the law, in all activities inherent in the company's operations, and in particular in the area of sensitive activities, keeping abreast of relevant regulatory developments;

- verify the trustworthiness of suppliers and any business and financial partners, based on certain relevant indices (e.g., public prejudicial data or acquisition of business information about the company, shareholders and directors);
- to be inspired by criteria of transparency in the exercise of corporate activity and in the choice of suppliers and any commercial and financial partners, paying the utmost attention to news concerning third parties with whom the Company has relationships of a financial or corporate nature that may even only generate the suspicion of the commission of one of the crimes de quo;
- Verify the regularity of collections/payments, with reference to the full coincidence between recipients/orderers of payments and counterparties actually involved in the transactions, indicating in distribution contracts who the payers are, if different from those in the name of the contracts, and under what economic and commercial agreements they assign the payment, and in the reasons for third-party payments the reference to the goods sold;
- Use bank transfer as the preferred instrument of collection and payment;
- Ensure the traceability of decision-making stages related to financial and corporate relationships with third parties or Group companies;
- Keep documentation to support financial and corporate transactions, taking all necessary security measures;
- to be inspired by criteria of transparency in the management of transactions between related parties, which should always be carried out in accordance with market standards;
- Promptly inform those in charge - in compliance with the provisions set forth in internal regulations - whenever there is knowledge, suspicion or reasonable grounds to suspect that money laundering transactions are being or have been carried out or attempted.

2.11 OFFENSES INVOLVING NON-CASH PAYMENT INSTRUMENTS

(Art. 25-octies.1 Legislative Decree 231/2001)

In order to prevent and impede the occurrence of crimes involving non-cash payment instruments, but not limited to:

- Use company payment instruments other than cash, which one has the availability of for reasons inherent to one's work, for purposes other than those for which they were assigned;
- Obtaining credentials to access online, corporate or third-party payment systems using methods or procedures that do not comply with internal or external regulations;

- Exploit any vulnerabilities or inadequacies in the security measures of the company's or third parties' computer or telecommunications systems in order to misuse non-cash payment instruments.

It is, likewise, made obligatory to:

- Comply with internal and external laws and regulations on the use of payment instruments and the circulation of public credit cards and stamps.
- Diligently guard non-cash payment instruments and passwords for access to payment systems, preventing third parties from misusing them
- Notify the A.U. and the O.d.V. of any loss or misappropriation of instruments of non-cash payments and passwords to access payment systems.

2.12 COPYRIGHT INFRINGEMENT OFFENSES

(Art. 25-novies, Legislative Decree 231/2001)

In order to prevent and impede the occurrence of crimes in the area of violation of the right copyright, by way of example only, it is prohibited to:

- Making illegal downloads or transmitting right-protected content to third parties authorship;
- Abusively reproduce or distribute phonograms or videograms of musical or audiovisual works;
- reproducing, transferring to another medium, distributing, communicating, presenting or demonstrating in public the contents of a database without having first obtained the necessary authorization from the legitimate owner of the copyright and/or right of economic exploitation of the database.

With reference to the purchase or use by the Company of any asset susceptible to protection under copyright law, Recipients are also required to obtain from the respective owners and/or licensors of the relevant rights of use over the assets in question, specific declarations designed to certify the following main circumstances:

- that they are the rightful owners of the economic exploitation rights to the assets being transferred or otherwise have obtained permission from the rightful owners to grant their use to third parties;
- To ensure that the assets being transferred or licensed for use do not infringe any intellectual property rights held by third parties;

- to undertake to indemnify and hold harmless the Company from any damage or harm of a pecuniary or non-pecuniary nature that may be caused to it as a result of the untruthfulness, inaccuracy or incompleteness of this statement.

2.13 CRIMES RELATING TO FORGERY OF INSTRUMENTS OR SIGNS OF RECOGNITION

(Art. 25-bis, paragraph 1 letter f) bis and paragraph 2 Legislative Decree 231/2001)

In order to prevent and impede the occurrence of crimes related to the forgery of instruments or signs of recognition, merely by way of example and not limitation, it is prohibited to:

- Counterfeit, alter, use trademarks or distinctive signs, domestic or foreign, of third parties' industrial property registered and protected as trademarks;
- Introduce into the territory of the State, in order to make profit, hold for sale, put up for sale or otherwise put into circulation industrial products with counterfeit or altered domestic or foreign trademarks or other distinctive signs;

With reference to the purchase or use by the Company of any asset susceptible to third-party industrial property protection, Recipients are also required to obtain from the respective owners and/or licensors of the relevant rights of use over the assets in question, specific declarations aimed at certifying the following main circumstances:

- that they are the rightful owners of the economic exploitation rights to the assets being transferred or otherwise have obtained permission from the rightful owners to grant their use to third parties;
- To ensure that the assets being transferred or licensed for use do not infringe any intellectual property rights held by third parties;
- to undertake to indemnify and hold harmless the Company from any damage or harm of a pecuniary or non-pecuniary nature that may be caused to it as a result of the untruthfulness, inaccuracy or incompleteness of this statement.

2.14 CRIMES AGAINST INDUSTRY AND TRADE

(Art. 25 bis1, Legislative Decree 231/2001)

In order to prevent and impede the occurrence of crimes against industry and commerce, including but not limited to:

- prevent or disrupt the operation of an industry or trade by using Violence to property or using fraudulent means;
- Engaging in acts of competition with violence or threats;
- Putting on sale or otherwise circulating in domestic or foreign markets industrial products with counterfeit or altered names, trademarks or distinctive signs, causing harm to domestic industry;
- Selling in business one movable thing for another;
- Hold for sale or otherwise put into circulation intellectual works or industrial products with domestic or foreign names, trademarks or distinctive signs likely to mislead the buyer as to the origin, source or quality of the work or product;
- Industrially manufacture or use objects or other goods by usurping an industrial property title or in violation thereof, having knowledge of its existence.

With reference to the purchase or use by the Company of any asset susceptible to industrial property protection, Recipients are also required to obtain from the respective owners and/or licensors of the relevant rights of use over the assets in question, specific declarations aimed at certifying the following main circumstances:

- that they are the rightful owners of the economic exploitation rights to the assets being transferred or otherwise have obtained permission from the rightful owners to grant their use to third parties;
- To ensure that the assets being transferred or licensed for use do not infringe any intellectual property rights held by third parties;
- to undertake to indemnify and hold harmless the Company from any damage or harm of a pecuniary or non-pecuniary nature that may be caused to it as a result of the untruthfulness, inaccuracy or incompleteness of this statement.

2.15 TAX CRIMES

(Art 25-quinquiesdecies, Legislative Decree 231/2001)

In order to prevent and impede the occurrence of tax crimes, by way of example only, Recipients are required to:

- Drawing up, providing or transmitting to the Tax Administration documents and/or data that are correct, complete, exact and responsive to reality, such as to configure a limpid description of the Company's fiscal and financial situation for the purpose of the exact fulfillment of tax and fiscal obligations;

- Maintain a conduct marked by the principles of fairness, transparency and cooperation with the Tax Administration, ensuring full compliance with the laws and regulations, in the performance of all activities aimed at the acquisition, processing, management and communication of data and information intended to allow a well-founded and truthful judgment for tax purposes on the Company's financial, economic, tax and fiscal situation. In this regard, Recipients are prohibited in particular from:
- Account for (or hold for the purpose of evidence to the tax authorities) and use in returns (relating to income and/or value-added taxes) fictitious passive elements, derived from invoices or other documents for objectively/subjectively nonexistent transactions, in order to evade income or value-added taxes;
- indicating less than actual assets or fictitious liabilities or fictitious credits and deductions in returns, carrying out objectively or subjectively simulated transactions, or making use of false documents or other fraudulent means suitable for hindering the assessment and misleading the tax authorities, in order to evade income tax or value-added tax;
- Failing to file one of the returns relating to income tax or income tax on the value-added or substitute tax return;
- Issue or issue invoices or other documents for objectively/subjectively nonexistent transactions in order to enable third parties to evade income or value-added taxes;
- Alter or otherwise inaccurately report data and information intended for the preparation and drafting of documents of a financial, economic, financial and taxation nature;
- Conceal or destroy all or part of accounting records or documents required to be kept - so as not to allow the tax authorities to reconstruct income or turnover - in order to evade income or value-added taxes or to allow third parties to evade them;
- Use undue or nonexistent credits in compensation
- not to simulously alienate or perform other fraudulent acts on one's own property/assets or on the property of others suitable to render ineffective in whole or in part the compulsory collection procedure, in order to evade the payment of income or value-added taxes or of interest or administrative penalties related to said taxes;
- illustrate data and information in such a way as to give a true and fair view of the financial, economic, financial and fiscal position of the Company;
- Make available to shareholders and other Corporate Bodies all documentation concerning the management of the Company and prodromal to the performance of any and all verification and control activities legally and statutorily attributed to the

aforementioned. In this regard, Recipients are particularly prohibited from engaging in conduct that materially prevents or otherwise obstructs the performance of control activities by shareholders and other Control Bodies through the concealment or destruction of documents or through the use of other fraudulent means.

2.16 CRIMES AGAINST CULTURAL HERITAGE

(Art. 25-septiesdecies and Art. 25-duodevicies Legislative Decree 231/2001)

In order to prevent and prevent the occurrence of crimes against cultural heritage, by way of example only, Recipients are required to:

- Adopt the necessary measures to ensure the protection of cultural heritage, and thus of cultural property - such as immovable and movable things that are of artistic, historical, archaeological, ethno-anthropological, archival and bibliographical interest and the other things identified by or under the law as testimonies having civilizational value - and of landscape property - that is, those properties and areas that present conspicuous features of natural beauty, uncommon beauty and in general those areas constituting an expression of the historical, cultural, natural, morphological and aesthetic values of the territory;
- Involve the Superintendence of Cultural Heritage for all activities that have as their object or otherwise have an impact, even indirectly, on the cultural property owned or available to the Company and comply with the provisions issued by the latter.

3 AREA A - RISK ANALYSIS

3.1 RISK OF MANAGING RELATIONS WITH THE PUBLIC ADMINISTRATION AND SUPERVISORY AUTHORITIES

3.1.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)
- Fraud to the detriment of the state or other public entity (Article 640, paragraph 2, no. 1, Penal Code);
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Misappropriation of money or movable thing (314 bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code);
- Computer fraud (Art. 640-ter, Penal Code).
- Computer crimes and unlawful data processing (Art. 24-bis Legislative Decree 231/2001)
- Computer documents (Art. 491-bis Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).
- Corporate crimes (Art. 25-ter Legislative Decree 231/2001)
- Hindering the exercise of the functions of public supervisory authorities (Art. 2638 Civil Code).

3.1.2 SENSITIVE ACTIVITIES

Management of relations of any nature with Public Administration and Supervisory Authorities, including inspection visits by public entities.

3.1.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;
- Commercial Sector;
- Quality Service

3.1.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- participation, where possible, of at least two representatives of the Company in the case of meetings with the Public Administration;
- Establishment of a method for collecting, verifying and approving documentation to be transmitted to counterparties, with the support of the relevant functions;
- information to any additional facilities or, in cases of necessity and urgency, to the Sole Administrator;
- Formalization of reporting on the relationship that has taken place, unless appropriate documentation is already prepared by the counterparty;
- signing, in compliance with existing powers of attorney, the acts or communications to be transmitted to the Public Administration / Supervisory Authority;
- during inspections by public officials and judicial police officers, obligation for representatives of the Company to operate with integrity, transparency and fairness;
- drafting, by the heads of the facilities involved in inspections and/or assessments, an informative report of the activity carried out during the inspection, containing, among other things, the names of the officials met, the documents requested and/or handed over, the individuals involved and a summary of the verbal information requested and/or provided.

3.2 RISK OF PROCUREMENT OF GOODS, SERVICES AND CONSULTING SERVICES

3.2.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001) - Both direct and instrumental area

- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).
- Corporate crimes (Art. 25-ter Legislative Decree 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Inducement not to make statements or to make false statements to the Authority judicial (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the Authority judicial (Art. 377-bis Penal Code).
- Crimes against the individual (Art. 25-quinquies Legislative Decree 231/2001)
- Illegal intermediation and exploitation of labor (Article 603-bis Penal Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
 - o Receiving stolen goods (Art. 648 Penal Code);
 - o Money laundering (Art. 648-bis Penal Code);
 - o Use of money, goods or utilities of illicit origin (Art. 648-ter Penal Code);
 - o Self-laundering (Article 648-ter.1 Penal Code).
- Crimes for the purpose of terrorism or subversion of the democratic order (Article 25-quater Legislative Decree 231/2001)
- Financing of conduct for the purpose of terrorism (Article 270-quinquies 1 of the Criminal Code).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Article 2, paragraphs 1 and 2-bis, Article 3, Article 4, Article 5, Article 8, Article 10, Article 10-quater and Article 11 of Legislative Decree No. 74/2000 (As amended in numbering by Legislative Decree 5/11/2024 No. 173).

3.2.2 SENSITIVE ACTIVITIES

1. Qualification and evaluation of suppliers;
2. Survey of the need for goods and/or services and/or works;
3. Definition of purchasing methods (private treaty, infungible goods);
4. Bid evaluation;
5. Issuance and dispatch of purchase orders/contract stipulation;
6. Management of passive contracts.

3.2.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium
- Purchasing department manager

3.2.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- Existence of an accredited supplier registry that is updated and maintained by adequate figures;
- Conducting periodic evaluations by the Chief Executive Officer, or his delegate, of the suitability of the service rendered by providers;
- Formal verification of the supplier's possession of the necessary technical-professional requirements and reliability and honorability, as well as any potential conflict of interest situations;
- Appointment of a committee to evaluate suppliers for purchases exceeding 40,000 euros, consisting of a representative of the Purchasing function to evaluate the economic component, a representative of the Company to evaluate the technical component, and a Head of Administration;
- carrying out a preliminary check on the counterparty for qualification purposes, including through a commitment to comply with the requirements of the Code of Ethics attached to the Company's Model 231 (signing of the "231 clause"); as well as, by way of example, evidence of valid DURC, declaration in lieu of anti-mafia certification may be requested from the supplier.
- Formal monitoring and periodic updating of the Supplier Registry in order to:
 - o Record any non-conformities found in the delivery of the good/service;
 - o Verify that the requirements for qualification are maintained;
- o formal definition of case histories that result in the exclusion of suppliers /professionals from the registry;

- in the case of non-standard purchases, i.e. with a value exceeding 40,000 euros, approval of the purchase request by appropriate authorization levels;
- definition of criteria and related procedures for evaluating the fairness of the economic value of the bid in relation to the prospective labor and safety costs with reference to the services covered by the contract and, if it appears abnormally low, the examination of the written justifications and related accompanying documentation requested from the bidder;
- Establishment of criteria for emergency purchases (e.g., for health and safety reasons);
- Definition of different methods of selection of suppliers / consultants / external professionals depending on the economic amount of the purchase, its characteristics, or the occurrence of specific circumstances;
- Use of bid evaluation criteria marked by transparency and, as far as possible, limitation of subjectivity criteria;
- Preparation by the participants in the evaluation committee of a statement in which the person certifies that he or she is not in a situation, even potential, of conflict of interest with respect to the supplier being evaluated;
- Participation of the relevant functions in the evaluation of bids received;
- Establishment of criteria and how to award the contract;
- standardized contractual provisions in relation to the nature and type of contract, including contractual provisions aimed at compliance with control principles/ethical rules and rules of conduct in the management of activities by the third party;
- definition of the, activities to be followed and the functions to be involved in the event of any deviations from the standardized contractual provisions (also with reference to compliance, in line with the applicable legal provisions and/or in any case with reference best practices, with the working conditions in terms of remuneration, working hours, vacations, rests, permits, leave protection of minors of non-working age, supervisory methods and housing situations possibly offered to staff employed in connection with the performance of contractual services), providing for the possibility of carrying out, in the presence of specific risk indicators, verification and audit activities on compliance with the contents of the above contractual clauses;
- definition, within the contract, of the fees to be paid for the service, consistent with the nature and complexity of the assignment / service, as well as the skills and experience of the consultant / professional;
- Approval of the contract by appropriate authorizing levels;
- in case of open contract: a) consistency check between contract and Work Order (WO); b) signing of WO;
- Identification of the corporate function(s) responsible for managing the procurement contract with indication of assigned role and duties;

- Issuance of approval for payment of the invoice upon verification of its consistency with the good/work/service received and PO/Contract;
- Verification, prior to the payment of invoices, aimed at ascertaining:
 - (i) the correctness and consistency of the contract / Purchase Order with respect to the agreed terms and conditions;
 - (ii) verification of the consistency of fees with the good/work/service requested;
 - (iii) consistency between the counterparty who provided the service (good/work/service/consulting), the counterparty named in the contract, and the counterparty who issued the invoice;
 - (iv) the correct application of the value-added tax percentage with respect to the object of purchase and its proper application to the taxable amount;
 - (v) the approval of the invoice;
 - (vi) the correspondence between the amount of the transfer and the amount of the invoice;
- Definition of the methods and criteria for recording debit notes or credit notes received from suppliers;
- Provision of a formalized process for vendor evaluation;
- verification of the actual performance of the service or receipt of goods before Arrange for a payment of more than 40,000 euros to a supplier.

3.3 COMMERCIAL MANAGEMENT RISK - USE OF PRODUCTS WITH PROTECTED TRADEMARKS OR SIGNS OF INDUSTRIAL PROPERTY - CUSTOMER ACQUISITION AND SUPPLIERS

3.3.1 CRIMES ABSTRACTLY CONCEIVABLE

- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Protection of Industrial Property (Art. 25 bis, paragraph 1 lett. f)bis Legislative Decree 231/01)
 - Counterfeiting, alteration or use of trademarks or distinctive signs or of patents, models, designs (Art. 473 Penal Code);
 - Introduction into the State and trade in products with false signs (Art. 474 Penal Code);
- Crimes against industry and commerce (Art. 25bis 1 L.D. 231/01)
- Disturbing freedom of industry and commerce (Art. 513 Penal Code)
- Unlawful competition with threats and violence (Art. 513 bis Penal Code)

- Fraud against domestic industries (Art. 514 Penal Code)
- Fraud in the exercise of trade (Art. 515 Penal Code)
- Sale of industrial products with false signs (Art. 517 Penal Code)
- Manufacture and trade of goods made by usurping industrial property rights (Art. 517 ter Penal Code)
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
 - Criminal conspiracy (art. 416 Penal Code);
 - Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).
- Corporate crimes (Art. 25-ter Legislative Decree 231/2001) - Both direct and instrumental area;
 - Bribery among private individuals (Art. 2635 Civil Code);
 - Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001);
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or benefits of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Inducement not to make statements or to make false statements to the Authority judicial (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the Authority judicial (Art. 377-bis Penal Code).

3.3.2 SENSITIVE ACTIVITIES

Business promotion activities, customer and supplier acquisition, material acquisition and marketing of company products.

3.3.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Head of Commercial Sector;
- Head of Purchasing;
- Quality Manager.

3.3.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as, by way of example:

- Defining roles, responsibilities, and methods for managing business relationships;
- Adoption of a procedure governing the process of identifying and acquiring customers and suppliers;
- Definition of how customer and supplier master records are created and managed,
- Preparation and sharing with the Sole Administrator of Management Reporting on a four-monthly basis, in order to represent the first note regarding the income and expenditure of the company's current accounts, together with the final balance of orders fulfilled, orders in the process of being fulfilled, and purchases made for services and goods already rendered by suppliers or in the process of being rendered;
- Verification of ownership of rights to use trademarks or distinctive signs protected by third-party industrial property.

3.4 ACCOUNTING AND BUDGET RISK

3.4.1 CRIMES ABSTRACTLY CONCEIVABLE

Instrumental risk area for crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)

- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).
- Corporate crimes (Art. 25-ter Legislative Decree 231/2001) - Both direct and instrumental area
- False corporate communications (Art. 2621 Civil Code);
- Misdemeanors (Art. 2621-bis Civil Code);

- Obstruction of control (Art. 2625 Civil Code);
- Transactions to the detriment of creditors (art. 2629 Civil Code);
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Art. 2, paragraphs 1 and 2-bis, Art. 3, Art. 4, Art. 5, Art. 8, paragraphs 1 and 2-bis, Art. 10, Art. 10-quater and Art. 11 of Legislative Decree No. 74/2000, as amended in numerical indication by Legislative Decree 173/2024).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or benefits of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Inducement not to make statements or to make false statements to the Authority judicial (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the Authority judicial (Art. 377-bis Penal Code).

3.4.2 SENSITIVE ACTIVITIES

1. General accounting records (e.g., recording invoices, credit notes etc.);
2. Determination and execution of provisions for estimated items and budget closing operations;
3. Drafting and approval of the Budget Statement.

3.4.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;
- Accounting and auditing services provider

3.4.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as, by way of example:

- Defining roles, responsibilities and methods for managing the chart of accounts;
- Adoption of a cash flow control procedure for corporate liquidity testing;
- compliance with an approval process for general ledger entries to ensure their proper recognition;
- obligation to record invoices or other accounting documents only against business facts that actually occurred and were duly documented;
- Verification of the complete, accurate and timely recording and accounting of invoices and other tax-relevant business documents/facts;
- Accounting monitoring of the correctness of the imputations made in general accounting during the closing fiscal year;
- Balancing and analysis of balance sheet and income statement balances;
 - Analysis of suspense items at the closure of transitional accounts;
 - Checks for completeness and accuracy of closing and adjusting/integrating/adjusting entries;
 - Authorization of any corrective entries (in case of squaring or abnormal balances) and validation of the assessment data needed for integration and rectification entries;
 - Compliance with the approval process for all general ledger entries;
 - Periodic verification of the tax treatment of services/supplies received;
 - Definition of how customer and supplier master records are created and managed,
 - Verification of consistency and matching between receipts received and active invoices issued;
 - Preservation/storage of accounting records and documents whose preservation is mandatory through digital modes or services that ensure their availability and integrity;
 - Verification of the completeness and accuracy of the data and information to be transmitted to the Parent Company, if any, in connection with its consolidation operations and subsequent authorization of the same;

- Preparation of specific budgets for the organization of each event, in Consideration of the value of the sponsorships received;
- Preparation and sharing with the Sole Administrator on a four-monthly basis, in order to represent the first note regarding the income and expenditure of the company's current accounts, together with the summary of orders fulfilled, orders in the process of being fulfilled, and purchases made for services and goods already rendered by suppliers or in the process of being rendered;
- Verification of the correct determination of the operating result;
- Approval of the annual budget by the Shareholders' Meeting;
- Verification of the complete and correct recording of the operating result than the information contained in the minutes of the Shareholders' Meeting;
- Execution of expense reimbursements only upon issuance of the relevant authorization;
- Consistency check between the travel expenses to be reimbursed and the relevant expense slips;
- Definition of limits for reimbursement of expenses incurred

3.5 FINANCE AND TREASURY RISK

3.5.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001) - Both direct and instrumental area
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Instrumental risk area for Corporate Crimes (Art. 25-ter Legislative Decree 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Inducement not to make statements or to make false statements to the judicial authorities (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the judicial authority (Art. 377-bis Penal Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)

- Money laundering (Art. 648-bis Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater Legislative Decree 231/2001)
- Financing of conduct for the purpose of terrorism (Article 270-quinquies 1 of the Criminal Code).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Art. 2, paragraphs 1 and 2-bis, Art. 3, Art. 4, Art. 5, Art. 8, paragraphs 1 and 2-bis, Art. 10, Art. 10-quater and Art. 11 of Legislative Decree No. 74/2000 as amended in numerical listing by Legislative Decree 173/2024)).
- Crimes related to non-cash payment instruments (Article 25-octies.1 Legislative Decree 231/2001)
- Misuse and forgery of non-cash payment instruments (Article 493-ter of the Criminal Code);
- Computer fraud (Article 640-ter of the Criminal Code).

3.5.2 SENSITIVE ACTIVITIES

1. Opening/Closing of current accounts;
2. Management of payments and collections;
3. Petty cash management.

3.5.3 CORPORATE STRUCTURES INVOLVED

- a) Sole Administrator;
- b) Administrative Presidium;
- c) Commercial Sector

3.5.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in Model 231 and its protocols - Recipients performing their duties within this area

are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as but not limited to:

- Formal authorization to open, modify and close current accounts by the Sole Administrator;
- Prohibition of making a payment in a country other than the country where the contract was executed or other than the country of residence of the parties;
- Formal authorization of payments;
- Execution of payments exclusively by bank transfer;
- execution of payment arrangements against the documentation produced and evidencing approval for payment of invoices payable, authorization for payment of salaries, authorization for reimbursement of expenses incurred in travel, etc;
- verification of correspondence, prior to making payments, between: i) the recipients of the payments and the counterparties actually involved in the transactions; ii) the payment arranged, the relevant available supporting documentation (e.g., invoice/other accounting document), and the amount contractually agreed upon;
- Conducting daily reconciliations of current accounts, as well as related formalization of the checks performed;
- Verification and monitoring of collections, (verification of consistency between active invoices issued and collections received);
- Monthly reconciliation with daily audits of bank accounts
- Verification of consistency and matching between receipts received and active invoices issued;
- prohibition of the use of cash for any collection, payment or funds transfer transaction (subject to any exceptions dictated by objectively verifiable operational/management needs, always for limited amounts and in any case within the legal limits);
- With reference to petty cash management:
 - o Definition of the types of payments that can be made through petty cash;
 - o Provision for periodic reconciliations of petty cash inventories with the cash movement register;
- Annual replenishment of the cash fund;
- Assignment of corporate credit cards to personnel selected in light of specific needs related to their assigned duties;
- Prior authorization of payments to be made by corporate credit card;
- Access to home banking only to specifically authorized personnel, through the use of codes issued by the token or by password;

- Formal definition of the steps to be taken to recover debts, through involvement of multiple functions and the Sole Administrator, where it is appropriate to evaluate the actions to be taken for bad debt positions.
- Accounting management using management software.

3.6 STAFF SELECTION, RECRUITMENT, EVALUATION, EMPLOYMENT, REMUNERATION AND INCENTIVE RISK

3.6.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001) - Both direct and instrumental area
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Instrumental risk area for Corporate Crimes (Art. 25-ter Legislative Decree No. 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Inducement not to make statements or to make false statements to the judicial authorities (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the judicial authority (Art. 377-bis Penal Code).
- Crimes against the individual (Art. 25-quinquies Legislative Decree 231/2001)
- Illegal intermediation and exploitation of labor (Article 603-bis Penal Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or utilities of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Employment of third-country nationals whose stay is irregular (Art. 25- duodecies Legislative Decree 231/2001)
- Employment of third-country nationals whose stay is irregular (Article 22, paragraph 12-bis, Legislative Decree No. 286/1998).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).

- Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater Legislative Decree 231/2001)
- Financing of conduct for the purpose of terrorism (Article 270-quinquies 1 of the Criminal Code).

3.6.2 SENSITIVE ACTIVITIES

1. Staff selection and recruitment;
2. Formulation of the economic offer in compliance with the labor laws in force;
3. Evaluation of personnel aimed at the disbursement of incentives and bonuses;

3.6.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;

3.6.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- Resource planning process for hiring that takes into account the need;
- Establishment and approval of a hiring and incentive budget;
- Verification, prior to the start of selection activities, of the consistency of recruitment with the budget;
- Definition of the minimum necessary requirements (profile) to fill the role;
- Verification, through various screening stages, of the consistency of applications with the defined profile;

- Preliminary internal and inter-agency search for a person who fits the outlined profile;
- Checking for possible conflicts of interest between the recruiter and the candidate;
- performance of preventive checks on the hiring of personnel aimed at preventing the occurrence of prejudicial situations that expose the Company to the risk of committing predicate offenses on the subject of corporate administrative liability (with particular attention to the existence of conflicts of interest/relationships such as to interfere with the functions of public officials, public service officers called upon to operate in relation to activities in which the Company has an interest, failure to possess, in the case of citizens of non-EU countries, a valid residence permit, etc.);
- conducting interviews with selected candidates aimed at assessing their aptitude and technical characteristics;
- Formalization of the evaluation and selection of the candidate to be hired;
- Formulation of the economic offer and conditions of placement and contractual framework;
- definition of the relevant level of remuneration in line with the quantity and quality of work performance required and referring to the provisions of the National or Territorial Collective Bargaining Agreements/reference pay scales (if any);
- Approval and signature of engagement letters by the licensed attorney;
- collection and storage in special databases at the Confindustria Human Resources Department of the documentation of applications received and letters of employment;
- clear definition of the objectives assigned to each employee and the corresponding remuneration, in accordance with the criteria of fairness and balance;
- Establishment of ways of evaluating and reporting on employee performance;
- Formalization, discussion and archiving of evaluations;
- Authorization of salary increases, career advancement, bonuses and benefits by the Evaluation Committee;
- Establishment of a formalized process for the payment of incentives in proportion to the degree of achievement of objectives;
- Verification of correspondence between incentives paid and reported performance.

3.7 ADMINISTRATIVE PERSONNEL MANAGEMENT RISK

3.7.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001) - Both direct and instrumental area
- Fraud to the detriment of the state or other public entity (Article 640, paragraph 2, no. 1), Penal Code);
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code);
- Computer fraud (Art. 640-ter, Penal Code).
- Instrumental risk area for Corporate Crimes (Art. 25-ter Legislative Decree No. 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Inducement not to make statements or to make false statements to the judicial authorities (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the judicial authority (Art. 377-bis Penal Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or benefits of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Crimes against the individual (Art. 25-quinquies Legislative Decree 231/2001)
- Illicit intermediation and exploitation of labor (Article 603-bis Penal Code).
- Computer crimes and unlawful data processing (Art. 24-bis Legislative Decree 231/2001)
- Computer documents (Art. 491-bis Penal Code).
- Employment of third-country nationals whose stay is irregular (Art. 25- duodecies Legislative Decree 231/2001)
- Employment of third-country nationals whose stay is irregular (Article 22, paragraph 12-bis, Legislative Decree No. 286/1998).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).

- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Art. 2, paragraphs 1 and 2-bis, Art. 3, Art. 4, Art. 5, Art. 10 and Art. 10-quarter of Legislative Decree No. 74/2000 as amended in numerical listing by Legislative Decree 173/2024).

3.7.2 SENSITIVE ACTIVITIES

1. Employee master data management (entering and editing master data, payroll, etc.);
2. Managing attendance, leave, vacation and overtime;
3. Salary processing and related posting;
4. Management of expense reimbursements to employees.

3.7.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;
- Provider of personnel management services

3.7.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- Administrative management of personnel outsourced to the professional firm of CdL;
- signing, in compliance with existing powers of attorney, communications to be transmitted to the relevant Social Security and Welfare Agencies, after verifying the completeness, accuracy and truthfulness of the data and information contained therein;

- communications required by law to the relevant agencies with reference to the persons hired and to file the relevant documentation by the outsourcer;
- Monitoring the timelines to be met for communications, reports and fulfillments to the relevant Social Security and Welfare Agencies;
- Definition of how to open and manage employee master records;
- Traceability of changes made to employee records and storage of supporting documentation in the employee's file;
- Attendance tracking methods, including through automated systems, that ensure traceability in accordance with applicable legal requirements;
- Authorization of absences, vacation, leave and overtime by the immediate supervisor;
- Formal provision for periodic audits of compliance with legal regulations on the performance of work in line with normal working hours and the enjoyment of vacation, rest, leave and leave, as well as provision for activities to be followed in the event of any deviations;
- Verification about the correctness and completeness of the data transmitted to the outsourcer;
- Monthly verification of the correctness of coupons prepared by the outsourcer;
- Formal authorization for payment of salaries by the Sole Administrator;
- Use of operational control mechanisms to ensure consistency between hours paid and hours worked and to avoid the payment of wages/salaries that are not due or only partially due;
- Prior authorization from appropriate authorization levels to requests for travel/out of duty;
- Granting of expense advances only upon formal request, approved in advance by the immediate supervisor;
- Provision for a formal credit card allocation process;
- Existence of a monthly spending limit for credit cards;
- formal definition of the types of reimbursable expenses, amount limits related to the various types of expenses;
- Management of the process of uploading and approving expense reports using a computer system that ensures data traceability and authorization levels. Reimbursement of expenses is approved in advance in the system by the employee's immediate supervisor;

- formalized checks, by the Administrative Presidium about the relevance of the expenses for which reimbursement is requested and the correspondence between what is reported in the expense reports and the receipts delivered;
- Verification of credit card statements, with reference to the merit of expenses incurred by the Administrative Dean (with respect to type and supporting documentation);
- Verification of expenses incurred and authorization for reimbursement.

3.8 INFORMATION SYSTEMS MANAGEMENT RISK

3.8.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)
- Computer fraud (Art. 640-ter, Penal Code).
- Computer crimes and unlawful data processing (Art. 24-bis Legislative Decree 231/2001)
- Computer documents (Art. 491-bis Penal Code);
- Unauthorized access to a computer or telecommunications system (Art. 615-ter Penal Code);
- Unauthorized possession, dissemination and installation of equipment, codes and other means of access to computer and telematic systems (Article 615-quater Penal Code);
- Illegal interception, obstruction or interruption of computer or telematic communications (Art. 617-quater Penal Code);
- Unauthorized possession, dissemination and installation of equipment and other means of intercepting, preventing or interrupting computer or telematic communications (Article 617-quinquies Penal Code);
- Computer extortion (Article 629.3 Penal Code);
- Damage to computer information, data, and programs (Article 635-bis Penal Code);
- Damage to information, data, and computer programs used by the state or other public agency or otherwise of public utility (Article 635-ter Penal Code);
- Damage to computer or telematic systems (Art. 635-quater Penal Code);

- Damage to computer or telematic systems of public utility (Art. 635-quinquies Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).
- Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater Legislative Decree 231/2001)
- Financing of conduct for the purpose of terrorism (Article 270-quinquies 1 of the Criminal Code).
- Copyright infringement crimes (Article 25-novies Legislative Decree. 231/2001)
- Violation of the rules on the protection of copyright and other rights related to its exercise (art. 171, co. 1, lett. a-bis, and co. 3, art. 171 bis, art. 171 ter, art. 171 septies and art. 171 octies, L. 633/1941).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Article 10 of Legislative Decree No. 74/2000 as otherwise numbered by Legislative Decree. 173/2024).
- Crimes related to non-cash payment instruments (Article 25-octies.1 Legislative Decree 231/2001)
- Misuse and forgery of non-cash payment instruments (Article 493-ter of the Criminal Code);
- Computer fraud (Article 640-ter of the Criminal Code).

3.8.2 SENSITIVE ACTIVITIES

1. Management of logical access to data and systems or documents with evidentiary value by internal and external users;
2. Backup management;
3. Management of computer software, equipment, devices, or programs (change management);
4. Network security management;
5. Allocation and use of information technology resources.

3.8.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative sector;
- Warehouse Sector;
- Quality Verification Sector
- IT Support

3.8.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- Regulation of the process under the "Information Security" procedure;
- Formal request for the creation / modification / deletion of users enabled to use the information systems;
- Definition of unique access passwords;
- provision for constant information flows to the ICT function regarding new hires, role changes or staff resignations;
- Establishment of criteria regarding the proper creation and management of passwords;
- Definition of unique access passwords;
- Obligation to periodically renew the password;
- provision for suspension of utilities following a predefined number of failed login attempts;
- Prediction of closing inactive sessions after a limited period of time;
- Assignment, to employees, of a named e-mail address;
- Periodic review of active users in order to ensure proper profiling and granting of system privileges;

- Support in the periodic extraction of active users to ensure proper profiling and granting of privileges to the system;
- Assignment of user access profiles according to assigned tasks;
- Formal authorization for remote connection;
- Verification, with the support of external providers, of the successful completion of operations by checking appropriate logs;
- Logging of systems access via unalterable log files;
- Periodic review of active users in order to ensure proper profiling and granting of system privileges;
- Access to log files restricted to authorized personnel;
- Periodic monitoring of logs (access and activity) related to privileged users including System Administrators;
- Provision of information flow to the ICT function in case of suspicious e-mail messages;
- Archiving of incoming and outgoing e-mail messages;
- verification by security scanner before opening messages of incoming electronic mail;
- Proper storage of documents/accounting records (where digitized and/or dematerialized) in order to prevent their concealment or destruction or to ensure traceability of the process;
- Definition of criteria for the execution of a backup plan;
- Provision of a periodic backup plan for data, files, programs, and operating systems;
- Conducting periodic recovery tests;
- Tracking of maintenance requests on information systems (evolutionary, corrective and routine);
- Use of segregated environments for development, testing and production (both logical and physical segregation);
- Formal establishment of a change management process (including formal authorization of maintenance work);
- Formal authorization of putting into production applications developed/modified by third parties;
- Inventorying ICT applications;
- Use of appropriate antivirus programs automatically updated on servers and clients;
- Updating antivirus programs to be installed on servers and clients;
- Provision of spamming, anti-phishing and anti-virus filters for e-mail servers;

- Application of spamming, anti-phishing and anti-virus filters for e-mail servers;
- Prohibition of using copyrighted works without having the necessary permissions;
- Use of firewalls to protect the internal network;
- Conducting periodic vulnerability assessment/penetration tests;
- Formal establishment of business continuity or disaster recovery plans;
- Provision of periodic reporting in order to detect network anomalies and related monitoring;
- Provision for periodic monitoring/control activities of the effectiveness and Operation of the information security management system;
- Periodic network security audits through vulnerability scanning and health checking activities;
- Use of cryptographic controls to protect of information
And regulation of cryptographic key management;
- Provision of formalized rules related to the management of IT security incidents and problems;
- Operational management of information security incidents and problems;
- Formal identification of individuals in charge of configuring network equipment;
- Formal authorization, by those in charge, of changes on network equipment;
- Establishment of resource allocation criteria and IT services;
- Definition of authorization levels for the allocation of IT resources and services;
- Cataloging of assigned IT resources and periodic verification of them;
- Use of assigned IT resources exclusively for work-related purposes;
- Proper storage of documents/accounting records (where digitized and/or dematerialized) in order to prevent their concealment or destruction or to ensure traceability of the process;
- provision of dual control for all payment and monetary funds transfer systems for amounts exceeding 40,000 euros, requiring the intervention of two different parties, neither of which can manage the process independently;
- Joint audits with the supplier in case of changes related to payment details;

- programming of user education and awareness activities regarding information security, phishing, phone scams, impersonation calls, and social engineering attacks;
- Validation by the ICT function of the remote connection;
- Remote connection via secure modes using VPN

3.9 MANAGEMENT CONTROL RISK

3.9.1 CRIMES ABSTRACTLY CONCEIVABLE

Instrumental risk area for crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)

- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Instrumental risk area for Corporate Crimes (Art. 25-ter Legislative Decree No. 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Self-laundering (Article 648-ter.1 Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).

3.9.2 SENSITIVE ACTIVITIES

1. Preparation of the interim budget on a quarterly basis;
2. Checking trends in fulfilled orders and fixed business costs

3.9.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;
- Commercial Sector

3.9.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as, by way of example:

- Formal definition of how and when to articulate the planning and control process;
- Order and inventory trend analysis activities for constant verification of production capacity and correspondence between costs incurred and goods and services acquired;
- Periodic monitoring of receipts and sales performance.

3.10 PROPERTY AND EVENT MANAGEMENT RISK

3.10.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Instrumental risk area for Corporate Crimes (Art. 25-ter Legislative Decree No. 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).

- Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater Legislative Decree 231/2001)
- Financing of conduct for the purpose of terrorism (Article 270-quinquies 1 of the Criminal Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or utilities of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).
- Inducement not to make statements or to make false statements to the judicial authorities (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the judicial authority (Art. 377-bis Penal Code).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001, Art. 8, paragraphs 1 and 2- bis and Art. 10 of Legislative Decree No. 74/2000, as renumbered by Legislative Decree 173/2024).

3.10.2 SENSITIVE ACTIVITIES

- Negotiation and conclusion of real estate leases;
- Management of property leases;
- Credit management.

3.10.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium.

3.10.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as, by way of example:

- Regulation of the process under the "Active Cycle" procedure;
- formalization of the process of definition e implementation of policies commercial;
- Definition and periodic updating of the price list based on market quotations of leases, with the involvement of the Sole Administrator;
- Verification and authorization of rental rates for buildings, auditorium and meeting rooms, and definition of maximum discount thresholds;
- Checking the fairness of the rental price of the buildings, auditorium and meeting rooms against market conditions;
- in case of a conflict of interest between the representative of Confindustria Servizi and the third party (e.g., suppliers, consultants, business partners, customers, etc.), the obligation to report it, to refrain from negotiating/managing the contract by delegating to another person/unit;
- Formal approval of the budget in compliance with existing delegations and powers of attorney;
- Use of standardized contractual provisions, including contractual provisions aimed at compliance with control principles/ethical and conduct rules in the management of activities by the third party or sharing with the Legislative Affairs Area of Confindustria to define the activities to be followed in case of any deviations;
- Involvement of the relevant functions in case of any changes that have occurred in the contract conditions;
- inclusion within the leases of specific contractual clauses such as: acknowledgement and commitment to compliance with Model 231 and the Code of Ethics adopted by the Company; obligation to use the premises, the internal and external accessories with the utmost diligence, respecting the decorum of the building; assumption of the obligations of traceability of financial flows in the case of contracts with PA;
- Approval of the contract by appropriate authorizing levels;
- Periodic monitoring of the proper execution of contracts;

- Checking the completeness and accuracy of the invoice against the content of the contract/order, as well as against the services provided;
- Formal authorization to issue the invoice;
- Definition of how to manage and record credit notes;
- Formal authorization of credit notes;
- Monitoring, by the appropriate corporate functions, of seniority Of credits for blocking orders if the credit limit is exceeded;
- formal assessment, in compliance with existing delegated powers, regarding any reminder actions to be taken, i.e., the involvement of the relevant legal department and any reasoned recourse to the use of the allowance for doubtful accounts;
- Provision of criteria, methods and approval levels for write-off and write-down of receivables;
- Use of management software for accounting and contract management.

3.11 EVENT AND SPONSORSHIP MANAGEMENT RISK

3.11.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code).
- Instrumental risk area for Corporate Crimes (Art. 25-ter Legislative Decree No. 231/2001)
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or utilities of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).

- Inducement not to make statements or to make false statements to the judicial authorities (Art. 25-decies Legislative Decree 231/2001)
- Inducement not to make statements or to make false statements to the judicial authority (Art. 377-bis Penal Code).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Article 8, paragraphs 1 and 2-bis and Article 10 of Legislative Decree No. 74/2000 as renumbered by Legislative Decree 173/2024).

3.11.2 SENSITIVE ACTIVITIES

1. Negotiation and contracting for event and sponsorship management;
2. Management of event contracts and sponsorships.

3.11.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;
- Commercial Sector

3.11.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as, by way of example:

- Regulation of the process under the "Active Cycle" procedure;
- Preliminary evaluation of the elements of the bid request and development of the bid proposal;
- in the event of a conflict of interest between the representative of Micromed S.r.l. and the third party (e.g. suppliers, consultants, business partners, customers, etc.), the obligation to report it, to refrain from negotiating/managing the contract by delegating to another person/unit;

- Formal approval of the offer for sale in compliance with existing powers of attorney and proxies;
- Use of standardized contractual provisions, including contractual provisions aimed at compliance with control principles/ethical rules and rules of conduct in the management of activities by the third party or sharing with the Legislative Affairs Area of Confindustria to define the activities to be followed in case of any deviations;
- Involvement of the relevant functions in case of intervening changes in contract conditions;
- Verification of the correctness and consistency of the contract with respect to the object of the contract, as well as the consistency of the fees with respect to performance;
- Verification of correspondence between performance and what is stipulated in the Contract;
- Checking the completeness and accuracy of the invoice against the content of the contract/order, as well as against the services provided;
- Verification of the progress of the cost status and relative capacity. In case of incapacity, reshaping of the budget, subject to the maximum expenditure limits, set in consideration of the sponsorships received for the organization of the specific event;
- Prior authorization of any extra-budgetary expenses by the of the Sole Administrator when there are specific reasons;
- Formal authorization to issue the invoice;
- Definition of how to manage and record credit notes;
- Formal authorization of credit notes;
- Monitoring, by the relevant corporate functions, of the seniority Of credits for blocking orders if the credit limit is exceeded;
- formal assessment, in compliance with existing delegated powers, regarding any reminder actions to be taken, i.e., the involvement of the relevant legal department and any reasoned recourse to the use of the allowance for doubtful accounts;
- Provision of criteria, methods and approval levels for write-off and write-down of receivables;
- Use of management software for accounting and contract management.

3.12 CORPORATE COMPLIANCE MANAGEMENT RISK

3.12.1 CRIMES ABSTRACTLY CONCEIVABLE

- Corporate crimes (Art. 25-ter Legislative Decree 231/2001)
- Unlawful influence of the assembly (Art. 2636 Civil Code);
- Obstruction of control (Art. 2625 Civil Code);
- Illegal distribution of profits and reserves (Art. 2627 Civil Code);
- Transactions to the detriment of creditors (art. 2629 Civil Code);
- False corporate communications (Art. 2621 Civil Code);
- Misdemeanors (Art. 2621-bis Civil Code);
- Bribery among private individuals (Art. 2635 Civil Code);
- Instigation of bribery among private individuals (art. 2635 bis Civil Code).
- Receiving, laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies of Legislative Decree No. 231/2001)
- Self-laundering (Article 648-ter.1 Penal Code).
- Organized crime offenses (Article 24-ter of Legislative Decree No. 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).

3.12.2 SENSITIVE ACTIVITIES

1. Managing the acts of the Chief Administrator;
2. Management of relations with corporate bodies and members.

3.12.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Sector Administration
- Accounting and auditing services provider

3.12.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- Definition of the procedures for convening and conducting the Assembly in Compliance with the adopted regulatory and statutory principles;
- Checks to ensure the regular convening of the Assembly of the Members, as well as the free formation of the will of the assembly;
- Formalization within the Bylaws of the manner in which voting rights are represented at the Meeting;
- verification of the right to participate in the Assembly, including by proxy;
- compliance with the requirements imposed by law to protect the integrity and effectiveness of the share capital in order not to harm the guarantees of creditors and third parties in general in this regard;
- Minutes of the meetings of the Members' Assembly;
- timely provision of the Company's management documents to the Auditing Company in order to enable these bodies to carry out the necessary checks;
- observance of the tasks, roles and responsibilities defined by the corporate organizational chart and the authorization system in the management of ordinary operations (distribution of dividends, management of shareholders' contributions, management of reserves, etc.) and, in general, of all operations that may in any way affect the integrity of the share capital;
- Formal authorization to carry out or propose ordinary transactions to the relevant corporate bodies;
- Authorization of ordinary share capital transactions.

3.13 TAX COMPLIANCE MANAGEMENT RISK

3.13.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against the Public Administration (Articles 24 and 25 Legislative Decree 231/2001)
- Fraud to the detriment of the state or other public entity (Article 640, paragraph 2, no. 1), Penal Code);
- Bribery and Incitement to Bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322, 322-bis Penal Code);
- Trafficking in unlawful influence (Article 346-bis, paragraph 2, Penal Code);
- Computer fraud (Art. 640-ter, Penal Code).
- Corporate crimes (Art. 25-ter Legislative Decree 231/2001)
- False corporate communications (Art. 2621 Civil Code);
- Misdemeanors (Art. 2621-bis Civil Code);
- Obstruction of control (Art. 2625 Civil Code).
- Receiving stolen goods, money laundering and use of money, goods or benefits of illicit origin as well as self-money laundering (Article 25-octies Legislative Decree 231/2001)
- Money laundering (Art. 648-bis Penal Code);
- Use of money, goods or utilities of illicit origin (Art. 648-ter Penal Code);
- Self-laundering (Article 648-ter.1 Penal Code);
- Computer crimes and unlawful data processing (Art. 24-bis Legislative Decree 231/2001)
- Computer documents (Art. 491-bis Penal Code).
- Tax crimes (Art. 25-quinquiesdecies Legislative Decree 231/2001)
- Tax crimes (Art. 2, paragraphs 1 and 2-bis, Art. 3, Art. 4, Art. 5, Art. 8, paragraphs 1 and 2-bis, Art. 10, Art. 10-quater and Art. 11 of Legislative Decree No. 74/2000 as renumbered by Legislative Decree 173/24).
- Organized crime offenses (Art. 24-ter Legislative Decree 231/2001)
- Criminal conspiracy (art. 416 Penal Code);
- Mafia-type associations, including foreign ones (Art. 416-bis Penal Code).

3.13.2 SENSITIVE ACTIVITIES

1. Determination of direct and indirect taxes;
2. Preparation, approval and submission of tax returns or payment forms;
3. Making payments related to direct and indirect taxes.

3.13.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administrative Presidium;
- Accounting and auditing services provider

3.13.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients carrying out their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a service contract - to mitigate the risk factors characteristic of this area, such as, by way of example:

- Assignment of tax management and calculation to consultants
External taxation;
- Monitoring the timelines to be met for communications, reports and fulfillments with the tax authorities, through the cooperation of external tax advisors;
- Monitoring of regulatory changes in taxation;
- Formal definition of the methods and criteria for determining taxes (direct and indirect);
- specific checks on activities preparatory to the processing of tax returns, which include conducting additional checks on the items intended to go into them;

- Analysis of the performance of accounts receivable and accounts payable compared with historical data, to the
In order to identify any abnormal situations;
- Verification of the completeness and correctness of the data necessary for the calculation of taxes, the correctness of the tax calculation, the correct completion of the relevant Declaration and Payment Forms, and the complete and correct accounting records;
- reconciliation checks about the correspondence of VAT amounts with the relevant general ledger accounts;
- Control and monitoring activities of tax-relevant documentation provided to the external consultant, if any;
- Verification of compliance with regulatory requirements with respect to any amounts brought in for compensation that VAT;
- Verification about the truthfulness and correctness of certifications supporting tax credits;
- Subsequent verifications about the proper accounting of taxes;
- Signing of Declaration and Tax Payment Forms;
- formal authorization
 - Of the contents of the Declaration and Payment Forms,
 - To the sending of the same to the tax authorities.
 - To the payment of taxes;
- Accounting management using management software that enables data extraction;
- Filing of tax documentation by the relevant functions.

3.14 CULTURAL PROPERTY MANAGEMENT RISK

3.14.1 CRIMES ABSTRACTLY CONCEIVABLE

- Crimes against cultural heritage (Art. 25-septiesdecies Legislative Decree 231/2001)
- Misappropriation of cultural property (Article 518-ter of the Criminal Code).
- Receiving stolen cultural property (Article 518-quater of the Criminal Code).
- Destruction, dispersal, deterioration, defacement, defacement, and illegal use of cultural or scenic property (Art. 518-duodecies, Criminal Code)
- Laundering of cultural property and devastation and looting of cultural and landscape property (Art. 25-duodevicies Legislative Decree 231/2001)

- Laundering of cultural property (Article 518-sexies of the Criminal Code).

3.14.2 SENSITIVE ACTIVITIES

- Leases of buildings having cultural significance;
- Organization of events and conferences.

3.14.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Administration Manager;

3.14.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients performing their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as by way of example:

- Request for permission from the Superintendence of Cultural Heritage in the case of maintenance work or activities that have a direct or indirect impact on property of cultural significance;
- Conclusion of specific insurance policies in case of space rental aimed at organizing exhibitions;
- provision of contractual clauses by which the tenant undertakes to comply with the provisions of Model 231 and the Code of Ethics adopted by the Company and to use the premises, internal and external accessories with the utmost diligence respecting the decorum of the building;
- Formalization of mutual obligations in a complex service contract entered into with Confindustria for the concession of space;
- Definition of responsibilities in cultural archive management;

- census of the works of art on the property with an indication of the related quotation.

4 AREA B - ENVIRONMENTAL AND SAFETY RISK ANALYSIS

4.1 MANAGEMENT RISK OF ENVIRONMENTAL ISSUES

In order to prevent and prevent the occurrence of environmental crimes, all Recipients are required to comply with national and international environmental protection regulations, as well as regulations issued by the relevant environmental authorities;

Consequently, all Recipients of the Model-each for their own specifically identified activities of competence-must implement the environmental protection measures adopted by the Company, as well as the fulfillment of the obligations of:

- Act in accordance with the powers and responsibilities expressly conferred and observe The provisions and instructions given for the purpose of environmental protection;
- Carry out periodic checks on the performance of plant and equipment in order to enforce compliance with the quali-quantitative emission limits contained in the permits;
- Perform internal audits in the manner and frequency defined by the Company;
- Immediately report any critical situations of which they become aware, taking direct action, in cases of urgency, within the scope of their skills and possibilities, to eliminate or reduce the resulting environmental risks;
- Participate in relevant training courses conducted by the Company;
- Contribute to the fulfillment of all obligations imposed by the competent authority or otherwise necessary for the protection of the environment.
- In addition, again with reference to the management of environmental issues, any behavior aimed at:
 - to the establishment of relationships with third-party companies that do not have adequate technical-professional characteristics or propriety or do not have all the necessary authorizations, for example, to carry out waste collection, transportation and disposal activities;
 - to entering into or maintaining contractual relationships (e.g., lease, loan, etc.) with parties known to incur violations of environmental regulations;
 - to the direct or indirect management of waste (collection, transportation, recovery, disposal, trade, brokerage) in the absence of authorization, registration or communication.

4.1.1 CRIMES ABSTRACTLY CONCEIVABLE

- Organized crime offenses (Art. 24-ter Legislative Decree 231/01)
- Criminal conspiracy (Article 416 of the Criminal Code).
- Mafia-type associations, including foreign ones (Article 416-bis of the Criminal Code).
- Environmental crimes (Art. 25-undecies Legislative Decree 231/01)
- Violation of regulations on the cessation and reduction of the use of ozone-depleting substances (Article 3, Paragraph 6 of Law 549/1993);
- Organized activities for illegal waste trafficking (452-quaterdecies c.p.);
- Unauthorized waste management activities (Article 256, paragraphs 1, 3 first and second sentences, 5 and 6 first sentence of Legislative Decree 152/2006);
- Illegal waste trafficking (Article 259, paragraph 1 of Legislative Decree 152/2006).

4.1.2 SENSITIVE ACTIVITIES

- Waste management;
- Management of atmospheric emissions;
- Fire

4.1.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Production Manager.
- Warehouse Manager

4.1.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients performing their duties within this area are required to comply with a series of specific and concrete controls - some of which are outsourced and performed on behalf of the Company by a third party bound by a contract of

service - to mitigate the risk factors characteristic of this area, such as but not limited to:

- Existence of checks on the technical and professional requirements of suppliers, including waste transport/disposal permits;
- Existence of a dedicated area for the temporary storage of hazardous waste (e.g., toner) that is properly segregated and provided with restrictions on access to unauthorized parties;
- execution of waste collection activities by homogeneous categories and prior identification of the types of waste allowed to the area used for temporary storage, whereby the waste must be deposited inside the respective bins or containers, marked with appropriate signs identifying the types of waste allowed (waste identification CER code);
- clear identification of the persons in charge of transporting, disposing and/or recovering the waste and carrying out specific checks regarding the verification of the data reported in the FIR;
- signing the contract with outsourcers providing services in the area of waste transportation and disposal, in compliance with the system of proxies and powers of attorney;
- Execution of a census of assets containing ozone-depleting substances and establishment of the relevant plan for cessation of use and/or maintenance controls or decommissioning of the asset, in accordance with current regulations;
- Use of third-party suppliers for the maintenance activity of F-GAS systems, possessing the necessary certifications as regulated by Regulation (EU) 2015/2067; Regulation (EC) No. 304/2008 for companies operating on fire-fighting systems that make use of fluorinated gases
- Submission of annual declaration (MUD) to the relevant Chamber of Commerce in case of hazardous waste disposal

4.2 OCCUPATIONAL HEALTH AND SAFETY PROTECTION RISK

4.2.1 CRIMES ABSTRACTLY CONCEIVABLE

- Manslaughter (Art. 589 Penal Code) and serious or very serious injury (Art. 590 Penal Code) due to negligence, inexperience or failure to comply with laws or regulations on health and safety in the workplace (Art. 25-septies Legislative Decree 231/2001- Manslaughter and serious or very serious culpable personal injury committed in violation of the rules on the protection of health and safety in the workplace)
- The cited violations can be caused by, as a significant but not exhaustive example:
 - Failure to train Personnel on the health and safety risks associated with their job duties
 - Failure to provide personal protective equipment deemed necessary as a result of the protective measures made explicit in the Risk Assessment Document
 - Failure to maintain plant or equipment from which was caused the serious injury.

4.2.2 SENSITIVE ACTIVITIES

- Moving loads weighing more than 50 kg to and from the warehouse;
- Use of pressure cylinders containing SF6, C3F8, C2F6 gases.
- Use of flammable chemicals in the production process
- Use of electrical system in the absence of maintenance

4.2.3 CORPORATE STRUCTURES INVOLVED

- Sole Administrator;
- Production Manager.
- Warehouse Manager
- Safety officers

4.2.4 EXISTING CONTROLS

In the performance of their respective activities/functions - in addition to the rules defined in the 231 Model and its protocols - Recipients performing their duties within this area are required to comply with a series of specific and concrete controls to mitigate the risk factors characteristic of this area, such as by way of example:

- Delivery of compulsory courses in accordance with Legislative Decree 81/08 for the various roles
Of the corporate prevention organization;
- Documented delivery of personal protective equipment for tasks that are required to be used according to the contents of the company's Risk Assessment Document;
- Periodic maintenance of the endotamponant gas adduction system;
- Verification of technical suitability of contractors or suppliers interacting with Micromed, from whose activities health and safety risks could arise.
- Verification according to legal periodicity of fire-fighting equipment, such as fire extinguishers, hose reels, etc.)
- Periodic verification of the grounding system
- Periodic verification of the lightning protection system

5 ANNEXES TO ORGANIZATIONAL MODEL 231

1. Regulations of the Supervisory Board
2. Code of Ethics and Conduct
3. Organization chart
4. Risk Assessment Document
5. List of predicate offenses