CA AUTO BANK S.P.A.
“ORGANIZATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE 231/01”
Approved by the Board of Directors of the
January 29, 2026

AUTO BANK

Sommario

DEFINITIONS

- "Supervisory Authorities": are the Public Authorities (pursuant to Article 2638 of the Civil Code) that carry out supervisory activities over the Company, such as the Bank of Italy, Consob and/or other Authorities (e.g. the Italian Data Protection Authority, the Italian Competition Authority, etc.);

- "CCSL": First level Specific Collective Labor Agreement currently in force and applied by CA Auto Bank;

- "Code of Conduct": the principles of "corporate ethics" recognised as its own and which the Company calls for compliance by all Employees, Corporate Bodies, Consultants and *Partner,* available on the website www.ca-autobank.com);

- "Board of Directors (also BoD)": the Board of Directors of CA Auto Bank S.p.A.;

- "Collaborators": the individuals who have collaborative relationships with the Company without subordination, commercial representation and other relationships which materialise in a professional service of a non-subordinate nature, whether continuous or occasional, as well as those who, by virtue of specific mandates and powers of attorney, represent the Company towards third parties, including the collaborators of *branches* foreign;

- "Consultants": the individuals who have collaborative relationships with the Company without any subordination to them and who are requested to provide a service in particularly complex matters, including consultants of *branches* foreign;

- "Recipients": the subjects to whom the provisions of the Model apply and listed in Section II, paragraph 1.4;

- "Employees": persons subject to the direction or supervision of persons who hold representative, administrative or management roles within the Company, i.e. all persons who have an employment relationship of any nature with the Company, as well as workers with quasi-subordinate employment contracts, including employees of *branches* foreign;

- "Legislative Decree 231/01": Legislative Decree 8 June 2001 n. 231, containing the "*Regulation of the administrative liability of legal entities, companies, and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of September 29, 2000.*", in the content in force from time to time;

- "CA Auto Bank": CA Auto Bank S.p.A. with registered office in Turin, Corso Orbassano n.367, which will also be referred to in this document as the "Company";

- "Suppliers": those who provide goods or services to CA Auto Bank, including suppliers of *branches* foreign;

- "Group": CA Auto Bank S.p.A. and the companies directly and indirectly controlled by it;
- "Drivalia": Drivalia S.p.A. with sole shareholder;
- "Reference Guidelines": the Guidelines for the construction of Models of Organization, Management and Control pursuant to Legislative Decree 231/01 approved by Confindustria on 7 March 2002 and subsequent amendments and additions;
- "Model": this Organization, Management and Control Model adopted pursuant to Articles 6 and 7 of Legislative Decree 231/2001;
- "Governing body": the Board of Directors of CA Auto Bank;
- "Corporate Bodies": the members of the Board of Directors and the Board of Auditors of CA Auto Bank;
- "Supervisory Body (also Organism or OdV)": the Body of the Entity equipped with autonomous powers of initiative and control, with the task of monitoring the adequacy, functioning and compliance of the Model as well as ensuring its updating;
- "P.A.": the Public Administration, including its officials and persons in charge of public services;
- "Partner": natural persons or legal persons (temporary business associations - ATI, *joint-venture*, consortia, etc.), with which CA Auto Bank enters into any form of collaboration regulated by agreement or the contractual counterpart(s) of CA Auto Bank, both natural persons and legal persons (for example suppliers, customers, etc.) where they are intended to cooperate continuously with the company in the context of the Sensitive Processes, including the partners of the *branches* foreign;
- "Sensitive Processes": activities of CA Auto Bank in which there is a risk of crimes being committed;
- "Instrumental Processes": activities of CA Auto Bank which, although not directly at risk of committing Crimes (such as *infra* defined), are nevertheless instrumental and/or functional to their commission;
- "Crimes": the Crimes to which the provisions of Legislative Decree 231/01 apply (including any future amendments);
- "Internal Control System" or "ICS": an internal control system designed to continuously detect, measure, and monitor the risks inherent in the activities of CA Auto Bank. This system is composed of internal regulations such as company procedures, documentation, and provisions relating to the company's hierarchical, functional, and organizational structure, and the management control system.
- "Service Company": companies that perform service activities for companies of the CA Auto Bank Group, including CA Auto Bank S.p.A. itself and other companies of the Group and companies of the shareholders' Group, through a specific service contract.

- *"Whistleblower"*: person who reports illegal conduct or violations pursuant to Legislative Decree 24/2023, of which he or she has become aware by virtue of his or her duties.

PREMISE

CA Auto Bank S.p.A. (hereinafter also "CA Auto Bank" or "Company" or "Bank"), controlled by Crédit Agricole Consumer Finance (in turn part of Crédit Agricole S.A.), was born from the agreements between the French Group and Stellantis, announced in 2021, as part of the reorganization of the two companies' financial partnerships.

CA Auto Bank is a digital bank specializing in sustainable mobility. Operating in 18 countries, it combines a wide range of financing, leasing, and mobility services with innovative and flexible banking products.

The Company is registered in the Register of Banks held by the Bank of Italy, ABI Code 3445. Furthermore, it is the parent company of the "CA Auto Bank" Banking Group, registered in the Register of Banking Groups and is also registered in the Single Register of Insurance Intermediaries (RUI) no. D000164561.

The CA Auto Bank Group operates by managing the following financial services:

- ***Wholesale Financing Financing:*** financial activities towards the network of *dealer* of the reference car brands;
- ***Retail Financing:*** financing *retail* to support producers' sales by cooperating with their brands;
- ***Long Term Rental:*** long-term rental business.

In addition, the Bank offers additional banking products such as, for example, Deposit Accounts, Non-finalized Loans and Credit Cards.

The companies belonging to the CA Auto Bank Group operate not only in Italy, but also in France; Spain; Portugal; Germany; Belgium; the Netherlands; Greece; Austria; Switzerland; the United Kingdom; Ireland; Poland; Denmark; Sweden; Norway; Finland; and Morocco. A reorganization process of the foreign subsidiaries is currently being implemented through mergers by incorporation into the parent company and the establishment of *branches*.

The Company, with resolution of the Board of Directors dated **December 17, 2007** has adopted the first edition of this Organization, Management and Control Model pursuant to and for the purposes of Legislative Decree no. 231 of 8 June 2001.

The currently valid edition is the one resulting from the update approved by resolution of the Board of Directors dated January 29, 2026.

1. Relations with controlled companies

CA Auto Bank, as the parent company, may provide services to Group Companies that may involve risky activities and operations as per the Sensitive/Instrumental Processes of this Model.

These relationships are regulated by specific intra-group contracts.

The provision of these services is in accordance with the Code of Conduct and the Model adopted by the Company and is governed by specific written contracts.

2. Relations with foreign subsidiaries and *branches* CA Auto Bank foreign

2.1. Relations with foreign subsidiaries

The foreign subsidiaries of CA Auto Bank, although not among the recipients of this Model, are required to observe the "*231 Guidelines*", containing rules of conduct that foreign subsidiaries undertake to adopt in carrying out their business activities, in order to mitigate the risk of committing conduct that, pursuant to Italian law, may constitute predicate crimes pursuant to Legislative Decree 231/01.

2.2. Relations with the *branches* foreign

As mentioned above, CA Auto Bank has established *branches* in France, Ireland, Belgium, Poland, Germany, Spain and Portugal.

The provisions contained in this Model also apply to *branches* foreign.

In particular, in order to ensure compliance by the *branches* foreign, of the provisions contained in this Model, CA Auto Bank guarantees continuous coordination and connection between the activities carried out by itself and by the *branches* foreign.

This coordination and coordination activity is also carried out through the establishment of continuous information flows between the Recipients operating within the Company and at the *branches* foreign, with reference to the activities included in the Sensitive and Instrumental Processes listed in this Model.

Furthermore, in order to ensure compliance with the provisions of the Model by the *branches* abroad, the Company guarantees:

- that the training activity referred to in Section III of the General Part of the Model is also provided to the representatives of the *branches* foreign;
- that the information flows towards the Supervisory Body also come from the representatives of the *branches* foreign;
- that the supervisory activities carried out by the Supervisory Body also include, within their scope, the activities falling within the Sensitive and Instrumental Processes carried out by the *branches* foreign.

3. Corporate Governance of CA Auto Bank

CA Auto Bank has a traditional corporate governance structure consisting of a Board of Directors and a Board of Statutory Auditors, which acts as the supervisory body.

The Board of Directors, composed of ten members eligible for re-election, holds office for three years and expires upon approval of the financial statements for the third year of operation. Since 2014, the Board of Directors has had its own Bylaws, which govern its qualitative and quantitative composition and operating procedures, supplementing the provisions of the law and the Company's bylaws.

Responsibility for the Internal Control System lies with the Board of Directors, which establishes its guidelines and periodically verifies its adequacy and effective functioning, ensuring that the main corporate risks are identified and properly managed by the CEO and management.

The Company has based its Internal Control System on the following main elements:

- Second and third level control functions: Compliance, Risk and Permanent Control and Internal Audit

- *Code of Conduct*, containing the rules of conduct and general principles that all internal and external subjects having directly or indirectly

  a relationship with the Company and with each of the subsidiaries that are part of the CA Auto Bank Group;

- *System of delegations and powers*, defined by the Board of Directors or the CEO, based on the relevance of the various organizational positions, in line with the assigned responsibilities and periodically updated in light of changes in the organizational structure;

- *Procedural system*, consisting of Company and Group procedures, operating instructions, and internal communications aimed at clearly and effectively regulating relevant processes and establishing operating methods and control measures for carrying out company activities.

The Board of Statutory Auditors is composed of three members and two alternates, whose terms of office last three financial years and expire on the date of the Shareholders' Meeting called to approve the financial statements for the third financial year. The Board of Statutory Auditors is responsible for overseeing the completeness, adequacy, functionality, and reliability of the internal control system and the Risk Appetite Framework (RAF).

The auditing of the accounts is entrusted to a statutory auditing firm, duly registered in the relevant register and meeting the legal requirements. The appointment is granted by the Shareholders' Meeting based on a reasoned proposal from the Board of Statutory Auditors. The auditing firm's mandate lasts nine years and ends with the Shareholders' Meeting approving the financial statements for the ninth year.

AUTO BANK

SECTION I

INTRODUCTION

1. Legislative Decree No. 231/01 and relevant legislation

On June 8, 2001, Legislative Decree 231/01 was enacted, pursuant to the mandate set forth in Article 11 of Law No. 300 of September 29, 2000. It entered into force on July 4, 2001, and brought domestic legislation regarding the liability of legal entities into line with several international conventions to which Italy has long been a party.

Legislative Decree No. 231 of 8 June 2001 (hereinafter the “Decree” or “Legislative Decree 231/2001”) introduced into our legal system the administrative liability of legal persons, companies and associations, including those without legal personality (hereinafter “Entities”), in the event of the commission or attempted commission of certain types of crimes or administrative offenses, in the interest or to the advantage of the Entity, by:

- individuals who hold representative, administrative or management roles within the Entity or within one of its Organizational Units with financial and functional autonomy, as well as natural persons who exercise, even de facto, the management and control of the same (so-called “Top Management”);
- subjects “Subjected” to the direction or supervision of the persons referred to in the previous point.

This is a liability which, although defined by the legislator as "administrative", presents the characteristics of criminal liability because:

- results from the commission of crimes;
- it is ascertained by the criminal judge (during a proceeding in which the procedural provisions relating to the accused apply to the Entity, where compatible).

The liability of the Entity, pursuant to the Decree, is in addition to and does not replace the (criminal) liability of the perpetrator of the crime: both the natural person and the legal entity will, therefore, be subject to criminal proceedings.

The sanctions provided for by the Decree against the Entities are: i) pecuniary sanctions, ii) interdictory sanctions, iii) confiscation of the price or profit of the crime, iv) publication of the conviction.

The **financial penalties.** They apply whenever the liability of a legal entity is established and are determined by the criminal judge through a system of "quotas." Specifically, in assessing the fine, the judge determines the number of quotas taking into account the seriousness of the offense, the degree of the entity's liability, and the actions undertaken to eliminate or mitigate the consequences of the offense and prevent the commission of further offenses. The amount of the quota is set by the Decree between a minimum of €258.23 and a maximum of €1,549.37 and is specifically determined based on the entity's financial and financial situation.

The **interdictory sanctions.** They can be applied to certain types of crimes and to the most serious cases. This translates into:

- in the ban from carrying out business activities;

- in the suspension and revocation of authorisations, licences or concessions functional to the commission of the offence;
- in the prohibition on contracting with the Public Administration (except to obtain the performance of a public service);
- in the exclusion from benefits, financing, contributions or subsidies and in the possible revocation of those granted;
- in the prohibition of advertising goods or services.

The interdictory sanctions do not apply (or are revoked, if already applied as a precautionary measure) if the Entity, before the opening declaration of the first degree hearing, has:

- compensated for the damage or repaired it;
- eliminated the harmful or dangerous consequences of the crime (or, at least, made efforts to do so);
- made available to the Judicial Authority, for confiscation, the proceeds of the crime;
- eliminated the organizational deficiencies that led to the crime, adopting organizational models suitable for preventing the commission of new crimes.

The confiscation consists of the State's acquisition of the price or profit of the crime, or the acquisition of sums of money, goods, or other assets of equivalent value to the price or profit of the crime. However, it does not involve that portion of the price or profit of the crime that can be returned to the injured party. Confiscation is always ordered by a conviction.

Furthermore, when confiscation is not possible, it may involve sums of money, goods, or other assets of equivalent value to the price or profit of the crime. Therefore, the so-called "equivalent" confiscation is also provided for in matters concerning the liability of criminal entities. That is, it is not necessary to identify the assets constituting the profit of the crime; simply determining their value is sufficient to proceed with the confiscation of assets of equivalent value.

The **publication of the sentence.** It may be imposed when the organization is subject to a disqualification sanction. It is carried out by posting in the municipality where the organization has its headquarters and by publishing it on the Ministry of Justice website.

The Decree provides for a form of exemption from administrative liability that applies when the entity demonstrates that, prior to the commission of the unlawful act, it adopted and effectively implemented an Organization and Control Model suitable for preventing crimes of the type that occurred.
The decree also specifies the requirements that the Models must meet. Specifically:

- identify the activities within which the crimes provided for by the Decree may be committed;
- provide specific protocols aimed at planning the formation and implementation of the institution's decisions in relation to the crimes to be prevented;
- identify ways of managing financial resources that are suitable for preventing the commission of such crimes;

- establish reporting obligations towards the Body responsible for supervising the functioning and compliance with the Models;
- introduce a disciplinary system suitable for sanctioning failure to comply with the measures indicated in the Model.

If the crime is committed by individuals holding representative, administrative, or management roles within the entity 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 the same, the entity shall not be liable if it proves that:

- the governing body adopted and effectively implemented, before the commission of the crime, a Model suitable for preventing crimes of the type that occurred;
- the task of monitoring the functioning and compliance with the Model and ensuring its updating has been entrusted to a body within the institution equipped with autonomous powers of initiative and control;
- the subjects committed the crime by fraudulently evading the Model;
- there was no omission or insufficient supervision by the Supervisory Body with regard to the Model.

However, if the crime is committed by individuals subject to the management or supervision of one of the entities listed above, the legal entity is liable if the commission of the crime was made possible by failure to comply with the management and supervision obligations. Such failure to comply is, in any case, excluded if the Entity, prior to the commission of the crime, adopted and effectively implemented a Model suitable for preventing crimes of the type that occurred.

For a description of the individual types of crime to which the legislation in question applies, please refer to the more detailed discussion contained in Annex A of this Model.

2. The function of the Model pursuant to Legislative Decree 231/01

The adoption of the Model, provided by law as optional and not mandatory, was considered by CA Auto Bank as a significant opportunity to implement an "active" prevention of crimes, through the strengthening of its own *Corporate Governance* and of the Internal Control System, as well as the dissemination of suitable ethical/behavioral principles.

CA Auto Bank has therefore adopted and subsequently updated this Organizational Model following a complex activity of identifying the areas exposed, directly or indirectly, to the risk of crime (Sensitive and Instrumental Processes) and their consequent proceduralization, with the aim of:

- adapt its organizational structure to the provisions of Legislative Decree 8 June 2001, n. 231;

- verify the measures already in place within the Company, in order to verify their effectiveness for the purposes of Legislative Decree 231/2001;
- standardize and strengthen the existing measures at CA Auto Bank in order to align them with Italian legislation, with particular reference to issues relating to the administrative liability of entities;
- verify the tools already used by the Company to combat violations of company procedures and rules of conduct and establish the relevant sanctioning instruments;
- to raise awareness among all those who operate in the name and on behalf of CA Auto Bank of the risk of committing an illegal act, the commission of which is clearly condemned by the Company as always contrary to its interests and principles, even when it appears to provide an immediate or even indirect financial advantage;
- intervene promptly to prevent or counter even the mere attempt to commit the crimes themselves, thanks to constant monitoring of company activity;
- improve the *governance* corporate and the image of the Company.

The Model identifies - in accordance with the Code of Conduct adopted by the Company, which forms an integral part of it - the rules and procedures that must be respected by all Recipients, i.e. by those, such as Employees, Corporate Bodies, Service Companies, Consultants and *Partner*, who operate on behalf of or in the interest of the Company in the context of Sensitive and Instrumental Processes for the commission of the crimes giving rise to liability pursuant to Legislative Decree 231/01.

All CA Auto Bank employees are subject to this Model, even if they operate abroad, whether temporarily or as a result of secondment.

The Supervisory Body, appointed for this purpose, ensures constant monitoring of the implementation of the Model, through monitoring activities and the possible imposition of disciplinary or contractual sanctions aimed at actively censuring any illicit behavior.

3. Reference Guidelines

In preparing this Model, CA Auto Bank was inspired by the Confindustria Guidelines, the ABI Guidelines, the Assilea Guidelines and the Guidelines of the Italian Consumer and Real Estate Credit Association (ASSOFIN), the principles of which are described in Annex B and referred to in the text of this Model.

It is understood that the Model, having to be drawn up with reference to the concrete reality of the Company, may well differ from the reference Guidelines which, by their nature, are of a general nature.

SECTION II

CONSTRUCTION OF THE MODEL

1. Principles and inspiring elements of the CA Auto Bank Model

In preparing this Model, in addition to the provisions of Legislative Decree 231/01, the procedures and control systems (identified during the "*as-is*") already operating in the company and deemed suitable to also serve as crime prevention measures and control over Sensitive and Instrumental Processes. In particular, the following were found to be operating at CA Auto Bank:

- the Code of Conduct, which expresses the principles of "corporate ethics" recognised as its own and which the Company calls for compliance by all Employees, Corporate Bodies, Consultants and *Partner*;
- the principles of *Corporate Governance*, which reflect the applicable regulations and the *best practices* international;
- the Internal Control System (ICS) (and therefore, company procedures, documentation and provisions relating to the company's hierarchical-functional and organizational structure and management control system);
- the second-level control activities carried out by the Risk & Permanent Control and Compliance, Supervisory Relations & Data Protection (including AML) functions as well as the third-level control activities carried out by Internal Audit;
- the rules relating to the administrative, accounting, financial and reporting;
- internal communication and staff training;
- the disciplinary system of which the CCSL;
- in general, the applicable Italian and foreign legislation (including, for example, laws on workplace safety).

1.1 Features of the CA Auto Bank Model

In line with the provisions of Legislative Decree 231/01, this Model is characterised by the elements of *effectiveness*, *specificity* and *actuality*.

The effectiveness

The effectiveness of an Organizational Model depends on its concrete suitability to prevent, or at least significantly reduce, the risk of committing the crimes set forth in Legislative Decree 231/01. This suitability is ensured by the existence of decision-making and preventive and subsequent control mechanisms capable of identifying anomalous transactions, reporting conduct falling within risk areas, and implementing the resulting tools for timely intervention. The effectiveness of an Organizational Model, in fact, also depends on the efficiency of the tools suitable for identifying "symptoms of unlawful conduct."

The specificity

Specificity is one of the elements that characterizes the effectiveness of the Model, pursuant to art. 6, paragraph 2, letters a and b.

The specificity of the Model is connected to the risk areas – and requires a census of the activities within which crimes may be committed – and to the processes of forming and implementing the organization's decisions in "sensitive" sectors.

Similarly, the Model must also identify suitable methods for managing financial resources, provide for disclosure requirements and an adequate disciplinary system, as well as take into account the company's characteristics and size, the type of business it carries out, and its history.

Current events

With regard to this aspect, a Model is suitable for reducing the risks of crime if it is constantly adapted to the characteristics of the company's structure and activity.

Effective implementation of the Model requires, pursuant to Article 7 of Legislative Decree 231/01, periodic verification and any modifications thereto if any violations are discovered or changes occur in the company's/entity's business or organizational structure.

Article 6 of Legislative Decree 231/01 assigns the task of updating the Model to the Supervisory Body, as it holds independent powers of initiative and control.

1.2 The definition of the CA Auto Bank Model

The Model was drafted taking into account the operational characteristics, organizational structure, and methods of carrying out corporate activities, as well as the requirements set forth in the Decree (Article 6, paragraph 2).

The preparation of this Model was preceded by a series of preparatory activities divided into different phases and all aimed at building a risk prevention and management system in line with the provisions of Legislative Decree 231/01 and inspired not only by the provisions contained therein, but also by the relevant Guidelines.

1) **Identification of Sensitive/Instrumental Processes ("*as-is analysis*")**

To identify the areas most likely to be at risk of crimes being committed and the ways in which they can occur, we examined company documentation (organizational charts, activities performed, key processes, organizational provisions, internal procedures, risk assessment documents, etc.) and interviewed key personnel within the company structure. We asked questions aimed at providing in-depth information on Sensitive and Instrumental Processes and their controls (existing procedures, documentability of operations and controls, segregation of duties, etc.).

In accordance with the provisions of the Decree and in accordance with the procedures outlined above, CA Auto Bank's risky activities have been identified, taking into account the Company's current operations and existing organizational structure.

The Sensitive/Instrumental Processes which, at present, could constitute an occasion or method for the commission of the types of crimes governed by the Decree are the following:

- Customer relationship management;
- Management of administrative obligations, relations with the Supervisory Authorities and the Public Administration and related inspection activities;
- Litigation management and relations with the Judicial Authority and management of settlement agreements;
- Management of purchases of goods and services (including consultancy);
- Selection and management of *partner* commercial;
- Personnel management and reward system;
- Management of expense reports and entertainment expenses;
- Financial flow management;
- Relationship Management *intercompany*;
- Management of non-cash payment instruments;
- Management and evaluation of customer credit;
- Accounting management, budget preparation and tax management;
- Information Security Management;
- Management of the prevention and protection system in the field of health and safety in the workplace;
- Management of activities with environmental impact;
- Management of assembly activities, capital transactions and other non-routine operations;
- Management of gifts, donations, events and sponsorships;
- Management of development activities;
- Management of activities *remarketing*;
- Management of internal and external communications (investors, advertising, etc.);
- Management of relationships with corporate bodies.

2) **Creation of the "gap analysis"**

On the basis of the existing controls and procedures in relation to the Sensitive and Instrumental Processes and the provisions and purposes of Legislative Decree 231/01, an analysis was carried out to detect any actions to improve the current Internal Control System (processes and procedures) and the essential organizational requirements for the definition of a "specific" organization, management and monitoring model pursuant to Legislative Decree 231/01.

3) **Preparation of the Model**

This Model is structured into sections containing general principles and rules of conduct, designed to prevent the commission of the crimes envisaged in Legislative Decree 231/01 and reported in Annex A.

With regard to the prevention of crimes not specifically addressed here, the measures set out in the Company's Code of Conduct and the provisions contained in the Model as a whole were deemed valid and adequate.

Additionally, CA Auto Bank has:

- identified the existing internal rules and protocols (formalised or otherwise) with reference to the Sensitive/Instrumental Processes identified as being at risk of Crime;
- provided for specific protocols aimed at planning the training and implementation of the institution's decisions in relation to the crimes to be prevented;
- identified the methods of managing financial resources suitable for preventing the commission of crimes;
- provided for reporting obligations towards the body responsible for supervising the functioning and compliance with the models;
- introduced a disciplinary system suitable for sanctioning failure to comply with the measures indicated in the Model.

1.3 The adoption of the CA Auto Bank Model and its subsequent amendments

This Model was adopted by resolution of the Board of Directors of CA Auto Bank, which also established the Supervisory Body.

The current version of the Model was approved by resolution of the Board of Directors dated January 29, 2026.

Each member of the Board of Directors, as well as the Board of Statutory Auditors of the Company, has undertaken to comply with this Model.

Since this Model is a document issued by the governing body (in compliance with the provisions of art. 6, paragraph I, letter a) of Legislative Decree 231/01), any amendments and additions are the responsibility of the Board of Directors.

The Board of Directors may delegate specific changes to the Chief Executive Officer, provided that any changes made must be ratified annually.

1.4 The implementation of the Model CA Auto Bank

The principles and provisions of this document must be respected by:

- members of the Board of Directors and the Board of Statutory Auditors;
- attorneys and delegates acting in the name and on behalf of the Company;
- Employees and managers;
- Consultants, Collaborators and Suppliers, to the extent that they may be involved in carrying out activities in which the commission of one of the predicate crimes referred to

in the Decree is conceivable and who do not have their own Organizational Model for the specific part of reference;

- *Partner* as well as by all third parties acting in the name and on behalf of CA Auto Bank;
- those who act under the direction or supervision of company management within the scope of the tasks and functions assigned to them.

The subjects thus identified are hereinafter referred to as “Recipients”.

The responsibility for the implementation of this Model in relation to the Sensitive and Instrumental Processes identified lies exclusively with CA Auto Bank, which has assigned its Supervisory Body the responsibility of carrying out the relevant controls according to the procedures described in the Model itself.

2. The Supervisory Body

2.1 Identification of the Supervisory Body: appointment and dismissal

The Company has assigned the task of monitoring the functioning and compliance with the Model to the Supervisory Body (also known as the Supervisory Body) in order to ensure effective and efficient implementation of the Model.

The members of the Supervisory Body meet the requirements set out in the Guidelines of the Trade Associations and in particular:

- **autonomy and independence.**The Supervisory Body must remain free from any form of interference or pressure from operational management and must not be involved in any way in the performance of operational activities or management decisions. The Supervisory Body must not be subject to conflicts of interest, and neither the Supervisory Body as a whole nor its individual members must be assigned operational tasks that could undermine its autonomy. The requirement of autonomy and independence must also be understood as the absence of family ties or hierarchical dependencies with the Company's top management or with individuals holding operational powers within the Company. The Supervisory Body must report to the highest operational management of the company and must be able to communicate with them on an equal footing, acting as a "staff" with the Board of Directors.
- **honorability**This requirement is defined in relation to the provision of causes for ineligibility, revocation, suspension, or forfeiture from the function of Supervisory Body, as specified below.
- proven**professionalism**The Supervisory Body has specific capabilities in inspection and consultancy activities, as well as adequate technical and professional skills to perform the functions of analysis of control systems and of legal and criminal law nature. The Company considers the careful examination of the curricula of potential candidates and their previous experiences, favoring profiles who have developed specific professionalism in the field.
  As a rule, in carrying out its supervisory and control tasks, the Supervisory Body is supported by the Compliance, Supervisory Relations & Data Protection, Legal Affairs, Internal Audit and, where necessary, by the Risk & Permanent Control Function of CA Auto Bank.

- **continuity of action**The Supervisory Body continuously carries out the activities necessary for the supervision of the Model with adequate commitment and the necessary investigative powers, meeting at least quarterly. The Supervisory Body itself is responsible for defining aspects pertaining to the continuity of the Supervisory Body's action, such as the scheduling of activities, the recording of minutes of meetings, and the regulation of information flows from company structures. This responsibility is governed by a specific Regulation.
- **availability of organizational and financial resources necessary** for the performance of its functions. The independence of the Supervisory Body is also ensured by the allocation by the Board of Directors of an annual spending budget for the performance of its duties (e.g., specialist consultancy, travel, etc.). However, the Supervisory Body may independently commit resources that exceed its spending powers if their use is necessary to address exceptional and urgent situations. In such cases, the Body must inform the Board of Directors without delay.

The requirements described above must be verified at the time of appointment by the Board of Directors.

Internal or external members may be appointed to the collegial Supervisory Body, provided that each meets the aforementioned autonomy and independence requirements. In the case of a mixed composition, since internal members cannot be expected to be completely independent from the body, the degree of independence of the body must be assessed as a whole.

The appointment of the Supervisory Body and the removal of its mandate are the responsibility of the Board of Directors, which may delegate the Company's legal representatives to provide any necessary replacements in the event of the Supervisory Body's resignation and/or organizational changes, reporting to the Board of Directors itself, which must ratify any new appointment.
In order to enhance the independence requirement, the Supervisory Body of CA Auto Bank is composed of three members, two internal and one external.

With regard to internal members, the role is assigned, by resolution, to the Head of Compliance, Supervisory Relations & Data Protection and the Head of Internal Audit. The external member is an expert in 231/01 and criminal law.

The Supervisory Body holds office for the term approved by the Board of Directors and is eligible for re-election. The Board of Directors determines the Body's remuneration upon appointment for the entire term of office.

Causes of ineligibility, revocation, suspension and forfeiture

In appointing the members of the Supervisory Body, the Company's Board of Directors expressly took into account the following causes of ineligibility for the same members of the Supervisory Body.

The following cannot be elected:

- those who have been convicted with a sentence, even if not definitive, or with a sentence applying the penalty upon request (so-called plea bargaining) and even if with a conditionally suspended sentence, without prejudice to the effects of rehabilitation:
    1. to imprisonment for a period of not less than one year for one of the crimes provided for by Royal Decree 16 March 1942, n. 267;
    2. to a prison sentence of not less than one year for one of the crimes provided for by the provisions governing banking, financial, securities, insurance activities and by the provisions regarding markets and securities, payment instruments;
    3. to imprisonment for a term of not less than one year for a crime against public administration, against public faith, against property, against the public economy, or for a crime relating to tax matters;
    4. for any non-culpable crime, to the penalty of imprisonment for a term of not less than two years;
    5. for one of the crimes provided for in Title XI of Book V of the Civil Code as reformulated by Legislative Decree 11 April 2002, n. 61;
    6. for a crime which entails and has entailed a conviction to a penalty resulting in a ban, even temporary, from holding public office, or a temporary ban from holding managerial positions in legal entities and businesses;
    7. for one or more crimes among those specifically provided for by the Decree, even if with sentences of lesser penalties than those indicated in the previous points;
- those against whom one of the preventive measures provided for by Article 10, paragraph 3, of Law No. 575 of 31 May 1965, as replaced by Article 3 of Law No. 55 of 19 March 1990 and subsequent amendments, has been definitively applied;
- those against whom the additional administrative sanctions provided for by art. 187 have been applied*quarter*Legislative Decree 24 February 1998, n. 58.

The members of the Supervisory Body certify, through a self-certification, that they are not in any of the above-mentioned conditions, and expressly undertake to communicate any changes to the content of such declarations.

Any revocation of members of the Body must be decided by the Company's Board of Directors and may only be effected for reasons related to serious breaches of the mandate undertaken, including violations of the confidentiality obligations indicated below, as well as for the intervening causes for forfeiture listed below.

The members of the Supervisory Body **they decay** furthermore from the position at the time in which, following their appointment:

- have been convicted by a final sentence or by plea bargain for one of the crimes indicated in numbers 1, 2, 3, 4, 5, 6 and 7 of the conditions of ineligibility indicated above;
- have violated confidentiality obligations strictly connected to the performance of their duties;

- with reference only to the internal members of the Supervisory Body, their employment relationship with CA Auto Bank has ceased (following dismissal or resignation).

The members of the Supervisory Body are also **suspended** from the exercise of functions in the event of:

- conviction with a non-final sentence for one of the crimes indicated in numbers 1 to 7 of the conditions of ineligibility indicated above; application, upon request of the parties, of one of the penalties referred to in numbers 1 to 7 of the conditions of ineligibility indicated above;
- application of a personal precautionary measure;
- provisional application of one of the preventive measures provided for by Article 10, paragraph 3, of Law No. 575 of 31 May 1965, as replaced by Article 3 of Law No. 55 of 19 March 1990 and subsequent amendments.

The remuneration of the Body is determined by the Board of Directors at the time of appointment for the entire duration of the office.

2.2 Functions and powers of the Supervisory Body

The Supervisory Body is entrusted with the task of supervising:

- on compliance with the Model by the Recipients, in order to ensure that the defined rules and the measures put in place are followed as faithfully as possible and are in practice suitable for preventing the risks of the commission of the crimes highlighted;
- on the effectiveness and adequacy of the Model in relation to the company structure and the actual capacity to prevent the commission of crimes;
- so that the Code of Conduct and all the provisions contained therein are respected by all persons operating in any capacity within the Company;
- on the correct functioning of the control activities for each risk area, promptly reporting anomalies and malfunctions of the Model, following a comparison with the areas/functions involved

To this end, the Supervisory Body is guaranteed free access – across all Company functions, without the need for prior consent – to any information, data, or company document deemed relevant to the performance of its duties and must be constantly informed by management: a) on aspects of the company's business that may expose CA Auto Bank to the risk of committing one of the crimes; b) on relationships with Service Companies, Consultants, and Partners who operate on behalf of the Company in the context of Sensitive Transactions; c) on the Company's extraordinary transactions.

In particular, the Supervisory Body:

- verifies compliance with the methods and procedures set out in the Model and identifies any behavioral deviations that may emerge from the analysis of information flows and the reports to which the managers of the various functions are required to submit;

- interprets the relevant legislation (in coordination with the function responsible for managing Legal Affairs) and verifies the adequacy of the Model to such regulatory requirements;
- makes proposals to the management body for any changes and/or additions that may become necessary as a result of significant violations of the provisions of the Model, significant changes to the internal structure of the Company and/or the methods of carrying out business activities, as well as regulatory changes;
- reports to the governing body any confirmed violations of the Organizational Model that may lead to the institution's liability and coordinates with company management to evaluate the adoption of any disciplinary sanctions, without prejudice to the latter's responsibility for imposing the sanction and the related disciplinary procedure;
- coordinates with the head of the Human Resources function to define training programs for staff and the content of periodic communications to be made to Employees and Corporate Bodies, including through the Company's Intranet space, aimed at providing them with the necessary awareness and basic knowledge of the legislation referred to in Legislative Decree 231/01;
- informs the Board of Directors of any need to update the Model, where there is a need to adapt it in relation to changed company, regulatory and jurisprudential conditions.

The activities carried out by the Supervisory Body cannot be scrutinized by any other corporate body or structure, although the management body is in any case required to monitor the adequacy of its intervention, as the management body bears ultimate responsibility for the functioning of the Organizational Model.

2.3 Reporting from the Supervisory Body to top management

In order to guarantee its full autonomy and independence in carrying out its functions, the Supervisory Body reports directly to the Board of Directors and the Board of Statutory Auditors of CA Auto Bank and reports on the implementation of the Model and the emergence of any critical issues, through two lines of communication.*reporting:*

- the first, per event, on a basis **continuous**;
- the second, at least annually, through a written report that precisely indicates the activity carried out during the period, both in terms of checks carried out and the results obtained, and in relation to any need to update the Model.

Should the Supervisory Body detect critical issues attributable to any member of the Board of Directors or the Board of Statutory Auditors, the corresponding report must be promptly forwarded to one of the other non-involved parties.

Meetings with the bodies to which the Supervisory Body reports must be minuted, and copies of the minutes must be kept by the Supervisory Body and the bodies involved from time to time.

The Board of Statutory Auditors, the Board of Directors and the Chief Executive Officer have the right to convene the Supervisory Body at any time to report on particular events or situations relating to the functioning of and compliance with the Model.

The Supervisory Body, in turn, has the right to request to be heard by the Board of Directors whenever it deems it appropriate to interact with said body, or to request clarifications and information from the same Body.

2.4 Information flows to the Supervisory Body

The Supervisory Body is the recipient of any information, documentation and/or communication, including from third parties, relating to compliance with the Model.

All Recipients of this Model are required to provide information to the Supervisory Body, to be carried out following:

a) reports;

b) information.

The Supervisory Body of CA Auto Bank ensures **maximum confidentiality** in relation to any news, information, report, **under penalty of revocation of the mandate and the disciplinary measures defined below**, without prejudice to the needs inherent in carrying out investigations in the event that the support of external consultants to the Supervisory Body or other corporate structures is necessary.

The information, reports and *t*he documents provided for in this Model are kept by the Supervisory Body in a specific electronic and paper archive, in compliance with the legislation in force regarding the unlawful processing of personal data: the documents of the Supervisory Body must be kept at the Company's offices and contained in separate and closed cabinets, accessible only to its members and only for reasons connected to the performance of the tasks described above,**under penalty of immediate dismissal from office**.

a) The reports

The Model, as expressly provided for by the Decree, must establish information obligations towards the Supervisory Body.

All Recipients are required to promptly report to the Supervisory Body any deviation, violation, or suspected violation of which they are aware of the behavioral rules set out in the Company's Code of Conduct, as well as the principles of behavior and methods of carrying out the activities identified as "at risk" and governed by the Model.

In particular, any information relevant to compliance with and functioning of the Model must be communicated to the Supervisory Body, as well as any other information of any kind, including information from third parties, and pertaining to the implementation of the Model in the areas of activity at risk. and compliance with the provisions of the Code of Ethics.

To this end, reports to the Supervisory Body can be sent to the email address established for this purpose by CA Auto Bank S.p.A.:

organismodivigilanza@ca-autobank.com

or, alternatively, send by regular mail to the address:

Supervisory Body of CA Auto Bank S.p.A.

Corso Orbassano n. 367 10137 Turin.

b) information

The following must be mandatorily transmitted to the Supervisory Body:

- provisions and/or information from judicial police bodies, or from any other authority, which indicate that investigations are being carried out, even against unknown persons, for the crimes;
- requests for legal assistance submitted by Managers and/or Employees against whom the Judiciary is proceeding for the crimes provided for by the legislation;
- reports prepared by the heads of other company functions, as well as by the Control Functions/Bodies (including the Auditing Firm), as part of their audit activities and from which facts, acts, events or omissions may emerge that are critical to compliance with the provisions of Legislative Decree 231/01;
- any findings and sanctions imposed by Supervisory Authorities and Public Bodies (Bank of Italy, Consob, Revenue Agency, Labor Inspectorate, INPS, INAIL, ARPA, ASL, etc.) following inspections carried out outside of ordinary monitoring activities;
- information relating to disciplinary proceedings carried out and any sanctions imposed pursuant to the Model (including measures taken against Employees) or the measures to close such proceedings with the related reasons;
- the summary tables of contracts awarded following national and European tenders, or through private negotiations;
- information relating to contracts awarded by public bodies or entities performing public utility functions;
- periodic reporting on health and safety at work;
- organizational changes and the evolution of activities relating to risk areas;
- the system of delegations and powers of attorney adopted by the Company;
- operations relating to share capital;
- the main elements of the extraordinary operations started and concluded;
- the stipulation or renewal of intra-group performance and service contracts;
- any significant deviations from the budget or spending anomalies that emerged from the authorization requests during the final accounting phase of management control.

In addition to the above information, further information flows to the Supervisory Body are provided for in the Special Part of the Model and reported in the summary table in Annex D of this Model.

The information flows must reach the Organization using the methods and addresses indicated above.

2.5 Information collection and storage

The information, reports and informations provided for in this Model are kept by the Supervisory Body in a specific archive (electronic or paper) for a period of 10 years, in compliance with confidentiality and privacy legislation.

Access to the database is permitted exclusively to members of the Board of Statutory Auditors, Directors and persons delegated by them.

3. Whistleblowing System

The reporting system in question is currently governed by Legislative Decree 10 March 2023 n. 24 (adopted in implementation of EU Directive 1937/2019, concerning the*"protection of persons reporting breaches of Union law"and of people who report violations of national legal provisions*"), which reformed Law 179/2017, which extended for the first time the protection of the "*whistleblower*" to the private sector, establishing specific obligations for entities in the Organization, Management and Control Models with particular reference to the protection of the whistleblower from any form of retaliation and/or discrimination.

With the entry into force of the aforementioned legislation, it was already established that the suitability of an organizational, management and control model also required the institution to provide one or more reporting channels suitable for guaranteeing, including through electronic means, the confidentiality of the identity of the whistleblower who intended to submit detailed reports of unlawful conduct, relevant pursuant to Legislative Decree 231/2001, of which he or she had become aware by virtue of the functions performed at the Institution (this is the content of Article 6, paragraph 2).Until the Decree), providing for protective measures that would protect the whistleblower from any discrimination or retaliatory measures suffered as a result of having made a report.
The recent reform introduced by Legislative Decree no. 24/2023 has profoundly changed the sector's regulations, unifying their scope of application to both the private and public sectors. More specifically:

- on the one hand, Legislative Decree 24/2023 **broadens the scope of objective application of the discipline**, which today, in general, is no longer limited to facts relevant pursuant to Legislative Decree 231/2001 but is extended to behaviors that harm the public interest or the integrity of public administrations or private entities pursuant to art. 2 of Legislative Decree no. 24/2023.

- on the other,**indicates new and additional types of whistleblower**, also including other subjects external to the public or private entity (specifically identified in Article 3 of Legislative Decree 24/2023, including, for example, self-employed workers, freelancers and consultants, shareholders, volunteers and paid and unpaid interns, etc.)

Furthermore, pursuant to Article 21 of Legislative Decree 24/2023, ANAC has the power to impose administrative pecuniary sanctions, specifically:

- from 10,000 to 50,000 euros when it ascertains that retaliation has been committed or when it ascertains that the report has been hindered or that an attempt has been made to hinder it or that the confidentiality obligation pursuant to Article 12 of the decree in question has been violated;
- from 10,000 to 50,000 euros when it finds that reporting channels have not been established, that procedures for submitting and managing reports have not been adopted, or that the adoption of such procedures does not comply with the provisions of the legislation; as well as when it finds that the verification and analysis of the reports received has not been carried out;
- from 500 to 2,500 euros, in the case referred to in Article 16[1], paragraph 3, of Legislative Decree 24/2023, unless the reporting person has been convicted, even in the first instance, for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial or accounting authority.

With specific reference to **the protection measures put in place in favor of the whistleblower**, both the new and the previous legislation include among them:

- the prohibition of retaliation against whistleblowers for reasons related, directly or indirectly, to the report;
- the possibility of communicating to external public authorities the fact of having suffered retaliation in the workplace due to having made a report and following the imposition of sanctions (the ANAC is required to inform the Labour Inspectorate for the measures under its jurisdiction);
- the nullity of the retaliatory acts suffered (such as dismissal, demotion, etc.), providing the whistleblower with the presumption in court (which, however, admits proof to the contrary) that the damage suffered by him is a direct consequence of the report or complaint made.

Following the enactment of Legislative Decree 24/2023, ANAC published, with Resolution No. 311 of 12 July 2023, Guidelines on the protection of persons reporting violations of EU law and the protection of persons reporting violations of national legislation. The Guidelines provide guidance on submitting external reports to the Authority and on their management, as required by Article 10 of Legislative Decree 24/2023.

---

[1]Article 16, paragraph 3 of Legislative Decree 24/2023 provides that: "*Except as provided in Article 20, when the criminal liability of the reporting person for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial or accounting authority is ascertained, even by a first-instance judgment, or his civil liability, for the same reason, in cases of willful misconduct or gross negligence, the protections referred to in this chapter are not guaranteed and a disciplinary sanction is imposed on the reporting or reporting person.*

Similarly, Confindustria, with reference to the new regulation whistleblowing, in October 2023, published the "Operational guide for private entities", with the aim of offering companies subject to the new requirements indications and operational measures suitable for responding to the needs outlined by the Decree, clarifying however that the possibility of adopting, in compliance with the reference regulatory framework, the most appropriate organizational solutions based on their own structure and governance.

In compliance with the provisions of the new Whistleblowing regulations, the CA Auto Bank Group:

- has adopted a Procedure for managing reports and protecting whistleblowers, which, illustrating the contents of the new regulation, defines the methods and timeframes for submitting and managing reports, as well as a User Manual for the online platform that illustrates its operating methods. For details, please refer to document 02G.07. Whistleblowing procedure and the related attachments;

- has prepared a privacy policy providing information regarding the processing of personal data provided in the context of whistleblowing reports;

- has informed company personnel of the establishment of reporting channels and the adoption of the aforementioned Whistleblowing Procedure;

- has informed the recipients of the Model and all the individuals identified by Legislative Decree no. 24 of 2023 as potential whistleblowers (e.g., volunteers, interns, consultants, individuals holding administrative, management, control, and supervisory roles, even if only de facto, etc.) that any discriminatory measures adopted against them as a result of reporting unlawful conduct and irregularities may be reported by them to the National Labor Inspectorate (including, where applicable, to the trade unions to which they belong) as well as to the ANAC, as provided for by Legislative Decree no. 24 of 2023 and the related Guidelines issued by the same Authority;

- He also informed the recipients of the Model and all other potential whistleblowers as identified above that dismissal and any other retaliatory or discriminatory measures adopted against them as a consequence of reports made are null and void and, in this sense, in the context of any subsequent employment law proceedings, a presumption is established in favor of the whistleblower (which admits proof to the contrary) that the imposition of measures against them was motivated by the submission of the report.

- has established specific internal channels, suitable for guaranteeing the confidentiality of the whistleblower's identity (as mentioned, with specific reference to the context of the Company, to be understood as unlawful conduct relevant pursuant to Legislative Decree 231/2001 or, alternatively, conduct carried out in violation of the provisions of the Group's Organizational Model).

With specific regard to reporting channels, the following have been identified:

- Internal channels within the CA Auto Bank Group

Specifically, the Group uses an internal platform (“BKMS”), made available by the Credit Agricole Group, through which it can process reports.

Reports can therefore be made, even anonymously, after having read the Privacy Policy pursuant to the GDPR (General Data Protection Regulation – EU Regulation 2016/679) through the following channels:

- By accessing the BKMS platform and/or accessing the CA Auto Bank hub corporate intranet in the "Code of Conduct" section. The platform guarantees the confidentiality of the reporting party, the facts, and the individuals involved in the report. The platform allows you to indicate the Group entity to which the report refers; by email to the following address: whistleblowing@ca-autobank.com; orally or in writing, with communication to the Head of Compliance, Supervisory Relations & Data Protection.

As a priority, whistleblowers are encouraged to use the Group's internal channels. Under certain conditions, they can file an external report directly to the competent authorities.

- Channels external to the CA Auto Bank Group

In Italy, it is possible to file an external report with the National Anti-Corruption Authority (ANAC) if one of the following conditions applies at the time of filing:

- the mandatory activation of the internal reporting channel is not foreseen within the work context or this is not active or, even if activated, does not comply with external regulations;

- the whistleblower has already made an internal report and it has not been followed up

- the whistleblower has reasonable grounds to believe that, if he or she were to make an internal report, it would not be followed up effectively or that the report itself could give rise to the risk of retaliation;

- have reasonable grounds to believe that the infringement may constitute an imminent or manifest danger to the public interest.

Reports external to ANAC can be made according to the methods established by ANAC itself

The Company, in compliance with the provisions of Legislative Decree no. 24/2023, has implemented a reporting system capable of protecting the identity of the whistleblower, the content of the reports, and their right to confidentiality. This includes the introduction of specific sanctions within the disciplinary system for any retaliatory acts or discriminatory behavior against the whistleblower for having reported, in good faith and on the basis of reasonable factual evidence, unlawful conduct and/or violations of the Organization, Management, and Control Model, as well as other violations indicated in Legislative Decree 24/2023.

Please refer to document 02G.07. Whistleblowing procedure for all specific references to reporting channels.

4. Checks on the adequacy of the Model

The Supervisory Body carries out periodic checks on the actual ability of the Model to prevent the commission of crimes, normally making use of the Compliance, Supervisory Relations & Data Protection Function, Internal Audit, the Risk & Permanent Control Function and the support of other internal functions that, from time to time, become necessary for this purpose.

This activity takes the form of random checks of the main corporate documents and most significant contracts concluded by CA Auto Bank in relation to the Sensitive and Instrumental Processes and their compliance with the rules set out in this Model, as well as the Employees' and Corporate Bodies' knowledge of the Company's Model and Legislative Decree 231/2001.

SECTION III

THE DIFFUSION OF THE MODEL

Knowledge of this Model is essential to developing the awareness of all Recipients who operate on behalf and/or in the interest of the Company within the scope of Sensitive and Instrumental Processes of the possibility of incurring unlawful acts that may result in criminally relevant consequences, not only for themselves but also for the Company, in the event of conduct contrary to the provisions of Legislative Decree 231/01 and the Model.

The Company guarantees correct and complete knowledge of the Model, the content of the Decree and the obligations arising from it among those who work for CA Auto Bank.

Training sessions will be organized over time by the Company, based on the criteria of mandatory and recurring training, as well as the potential need for diversification.

The Compliance, Supervisory Relations & Data Protection Function, having consulted the Supervisory Body, defines a specific communications and training plan annually, with the support of the Human Resources function.

1. Employee training and information

CA Auto Bank must ensure that both existing and new employees are provided with correct information/training on the content of this Model and the rules of conduct contained therein, with varying degrees of detail depending on the level of involvement of the same employees in the Sensitive and Instrumental Processes.

The information and training system is supervised and integrated by the activities carried out in this field by the Supervisory Body in collaboration with the head of the function delegated to manage Human Resources.

- ***The initial communication***

The adoption of this Model is communicated to all resources present in the company by the Function*Human Resources*.

New hires, on the other hand, are provided with an information set (e.g., Code of Conduct, CCSL, Organizational Model, Legislative Decree 231/01, etc.) in electronic format, which ensures they are equipped with the knowledge considered of primary importance.

All subsequent changes and information regarding the Model will be communicated to company resources.

- ***The training***

Participation in training activities aimed at spreading knowledge of the legislation referred to in the Decree, of the Organization, Management and Control Model, of the Code of Conduct is to be considered **mandatory.** To this end, a continuous *reminder* until the training is completed.

The training activities aimed at disseminating knowledge of the regulations pursuant to Legislative Decree 231/01 are differentiated, in content and delivery methods, based on the qualifications of the Recipients, the risk level of the area in which they operate, and whether or not they hold Company representation roles.

In particular, the Company has provided different levels of information and training through appropriate dissemination tools.

The Supervisory Body is also responsible for monitoring the content of the training programs as described above.

All training programs implemented by CA Auto Bank have a common minimum content consisting of the illustration, according to a modular approach, of the following elements:

- the relevant regulatory context;
- the characteristics and principles of the Organizational Model and the Code of Conduct;
- the main specific risks of the Bank, from a 231 perspective;
- the role and responsibilities of the Supervisory Body;
- the contact methods of the Supervisory Body and whistleblowing.

In addition to this common framework, each training program is tailored to provide its users with the tools necessary to fully comply with the provisions of Legislative Decree 231/01 in relation to the scope of operations and the tasks performed.

The Supervisory Body ensures that training programs are qualitatively adequate and effectively implemented.

2. Information for Service Companies, Consultants, Partners and Suppliers

The Company requires knowledge and compliance with the Model to Service Companies, Consultants, Collaborators,*Partner*and to Suppliers pursuant to specific contractual clauses. These parties must, in fact, be informed of the contents of the Model and of CA Auto Bank's requirement that their behavior comply with the provisions of Legislative Decree 231/01.

3. Information for Administrators and Mayors

This Model is delivered to each Director and Mayor, who undertake to comply with it.

SECTION IV

SANCTION SYSTEM

1. Function of the disciplinary system

The establishment of a system of sanctions (commensurate with the violation and designed to provide deterrence), applicable in the event of violation of the rules set forth in this Model, is intended to ensure the effectiveness of the Model itself. The establishment of this disciplinary and/or contractual sanctioning system constitutes, pursuant to Article 6, second paragraph, letter e) of Legislative Decree 231/01, an essential requirement of the Model itself for the purposes of exempting the Company from liability.

The system itself is intended to sanction: failure to comply with the principles and behavioral obligations set forth in this Organizational Model; violation of the measures established to protect those who report significant unlawful conduct pursuant to Legislative Decree 231/2001, or violations of the Corporate Organization, Management, and Control Model, as well as the conduct of those who make unfounded reports with intent or gross negligence.

The application of the disciplinary system and the related sanctions is independent of the conduct and outcome of any criminal proceedings initiated by the judicial authority in the event that the conduct to be censured also constitutes a relevant crime pursuant to Legislative Decree 231/01.

In any case, the right to claim compensation for any damages caused to the Company by conduct in violation of the rules set forth in this Model remains unaffected, as in the case of application by the Judge of the precautionary measures provided for by Legislative Decree 231/01.

Following notification to the Supervisory Body of the occurrence of one of the above-mentioned circumstances, an investigation procedure is initiated in accordance with the provisions of the CCSL applied by CA Auto Bank. This investigation procedure is conducted by the Supervisory Body itself, in coordination with the corporate bodies responsible for imposing disciplinary sanctions, taking into account the seriousness of the conduct, any recurrence of the misconduct, or the degree of guilt.

CA Auto Bank, through its designated bodies and functions, consistently, impartially, and uniformly imposes sanctions proportionate to the respective violations or conduct, in compliance with current provisions governing employment relationships. The disciplinary measures applicable to the various professional roles are listed below.

The disciplinary system is subject to constant monitoring and evaluation by the Supervisory Body and the Head of the function delegated to manage Human Resources, with the latter remaining responsible for the concrete application of the disciplinary measures outlined herein, upon any notification from the Supervisory Body and after consulting the hierarchical superior of the perpetrator of the censured conduct.

2. Measures against Non-Managerial Employees

2.1 Disciplinary system

Behaviours in violation of this Model by non-managerial employees subject to the*CCSL applied to the Company*constitute a disciplinary offence.

Workers will be subject to the measures - in compliance with the procedures set forth in Article 7 of Law No. 300 of 20 May 1970 (Workers' Statute) and any applicable special regulations - provided for by the sanctions system of the aforementioned first-level CCSL, and specifically:

- verbal warning;
- written warning;
- a lot;
- Suspension from work and without pay for up to three days; - dismissal, with or without notice.

All provisions of the CCSL remain in force - and are hereby referred to - including:

- the obligation – in relation to the application of any disciplinary measure – to first notify the employee of the charge and to hear the latter's defence;
- the obligation – except for verbal warnings – that the complaint be made in writing and that the measure be not issued until 5 days have elapsed from the notification of the charge (during which the employee will be able to present his justifications);
- the obligation to provide the employee with reasons and communicate the imposition of the measure in writing.

As regards the ascertainment of infringements, disciplinary proceedings and the imposition of sanctions, the powers already conferred, within the limits of their respective competence, to the management corporate.

In application of the principle of proportionality, the following disciplinary sanctions are provided for in detail depending on the seriousness of the infringement committed.

Verbal warning: applies in the case of the most minor shortcomings or non-compliance with the principles and rules of conduct set out in this Model, if such behaviour is related to a minor

non-compliance with the contractual provisions or the directives and instructions given by management or superiors.

Written warning: applies in the event of non-compliance with the principles and rules of conduct set forth in this Model, with respect to non-compliant or inappropriate behavior to a degree that can be considered, even if not minor, but in any case not serious, if said behavior is related to a non-serious non-compliance with the contractual provisions or with the directives and instructions given by management or superiors.

more not exceeding three hours of hourly pay calculated on the basic wage: applies in case of non-compliance with the principles and rules of conduct set out in this Model, for a**non-compliant or inappropriate behavior to** the provisions of the Model to such an extent as to be considered of **a certain gravity**, even if resulting from a repeat offense. Such behavior includes the violation of reporting obligations to the Supervisory Body regarding the commission of crimes, even attempted ones, as well as any violation of the Model. The same sanction will be applied in the event of repeated failure to participate (in person or in any way requested by the Company), without justifiable reason, in training sessions that will be provided by the Company over time regarding Legislative Decree 231/2001, the Organization, Management, and Control Model, and the Code of Conduct adopted by the Company, or regarding related topics. This sanction also applies in the event of a violation of measures protecting the whistleblower's confidentiality or of reports of unlawful conduct or violations of the Model or Code of Conduct that are found to be unfounded and made with intent or gross negligence.

Suspension from work and pay for up to three days: applies in the case of violations more serious than the infringements referred to in the previous point.

Dismissal with notice: applies in the event of serious and/or repeated violation of the rules of conduct and regulations contained in the Model, which do not conflict with the law and contractual provisions.

Dismissal without notice: This provision applies to workers who cause serious moral or material harm to the company or who, in connection with the performance of the employment relationship, carry out actions that constitute a crime under the law.

2.2 Violations of the Model and related sanctions

The following behaviors that constitute a violation of this Model are punishable:

- violations by the employee of internal procedures provided for by this Model or the adoption, in carrying out activities connected to the Sensitive and Instrumental Processes, of behaviors that do not comply with the provisions of the Model, whether or not they expose the Company to an objective situation of risk of committing one of the crimes;
- the adoption of behaviors that do not comply with the provisions of this Model and are aimed unequivocally at committing one or more crimes;

- the adoption of behaviors in violation of the provisions of this Model, such as to determine the actual and/or potential application against the Company of sanctions provided for by Legislative Decree 231/01;
- Violation of the measures established to protect those who report significant unlawful conduct pursuant to Legislative Decree 231/2001 or violations of the Organization, Management, and Control Model; - Submitting unfounded reports with intent or gross negligence.

The sanctions, of a disciplinary and contractual nature, and any request for compensation for damages, will be commensurate with the level of responsibility and autonomy of the Employee, or with the role and intensity of the fiduciary bond connected to the role conferred on the Directors, Auditors, Service Companies, Consultants, *Partners and* Suppliers.

The disciplinary system is subject to constant monitoring and evaluation by the Supervisory Body and the Head of the function delegated to manage Human Resources, with the latter remaining responsible for the concrete application of the disciplinary measures outlined herein upon any report from the Supervisory Body and after consulting the hierarchical superior of the perpetrator of the censured conduct.

3. Measures against Managers

Violation of the principles and rules of conduct contained in this Model by Managers, or the adoption of a conduct **not compliant with the aforementioned provisions**, as well as the violation of the measures to protect the *whistleblower* or the submission of unfounded reports, with intent or gross negligence, will be subject to the most appropriate disciplinary measure, in accordance with the provisions of art. 2119 of the Italian Civil Code and the Collective Bargaining Agreement applied by the Company.

In the most serious cases, termination of the employment relationship is envisaged, given the special bond of trust that binds the Manager to the employer.

The following also constitute a disciplinary offence:

- the failure of management to monitor the correct application of the rules set out in the Model by hierarchically subordinate workers;
- the violation of the obligations to inform the Supervisory Body regarding the commission of relevant crimes, even if attempted;
- violation of the whistleblower protection measures set forth in Law No. 179/2017;
- the submission of unfounded reports with malice or gross negligence;
- the violation of the rules of conduct contained therein by the managers themselves;
- the adoption, in the performance of their respective duties, of behaviors that are not in accordance with conduct reasonably expected of a manager, in relation to the role held and the degree of autonomy recognized.

4. Measures against the Administrators

In the event of conduct in violation of this Model by one or more members of the Board of Directors, the Supervisory Body shall inform the Board of Directors and the Board of Statutory Auditors, who shall take appropriate measures, including, for example, convening a shareholders' meeting in order to adopt the most appropriate measures permitted by law.

5. Measures against Mayors

In the event of violations of this Model by one or more Auditors, the Supervisory Body must immediately notify the Chairman of the Board of Directors through a written report. If the violations constitute just cause for dismissal, the Chairman of the Board of Directors shall convene the Shareholders' Meeting, forwarding the Supervisory Body's report to the shareholders in advance. The adoption of the measures resulting from the aforementioned violation is, in any case, the responsibility of the Shareholders' Meeting.

6. Measures against Service Companies, Consultants, Partners and Suppliers

Any conduct in violation of this Model by Service Companies, Consultants, including those in coordinated collaboration relationships, Collaborators, Partners, Suppliers, and anyone else included from time to time among the "Recipients" of the Model will be sanctioned in accordance with the specific contractual clauses included in the relevant contracts, and in any case with the application of conventional penalties, which may also include automatic termination of the contract, without prejudice to compensation for damages.

7. Measures against the Supervisory Body and other entities

The disciplinary and contractual sanctioning system identified above will also apply to the Supervisory Body or to those individuals, Employees or Directors, who, through negligence, imprudence or incompetence, have failed to identify and consequently eliminate behaviors that violate the Model.

SECTION V

THE CA Auto BANK ORGANIZATIONAL MODEL

1. General Control Environment

1.1 The Bank's organizational system

The Bank's organizational system complies with the fundamental requirements of formalization and clarity, communication, and separation of roles, particularly with regard to

the assignment of responsibilities, representation, definition of hierarchical lines, and operational activities.

The Bank's internal control system consists of the set of rules, functions, structures, resources, processes, and procedures that aim to ensure, in compliance with sound and prudent management, the achievement of the following objectives:

- verification of the implementation of the Group's strategies and policies;
- containment of risk within the limits indicated in the reference framework for determining the bank's risk appetite (Risk Appetite Framework - "RAF");
- safeguarding the value of assets and protecting against losses;
- effectiveness and efficiency of business processes;
- reliability and security of company information and IT procedures;
- prevention of the risk that the bank is involved, even unintentionally, in illicit activities (with particular reference to those connected with money laundering, usury and the financing of terrorism);
- compliance of operations with the law and supervisory regulations, as well as with internal policies, regulations and procedures.

The Bank is equipped with organizational tools (organization charts, organizational communications,*policy and* procedures, etc.) based on general principles of:

- knowability within the Company;
- clear and formal delimitation of roles and functions;
- - clear description of the reporting lines.

Internal procedures must be characterised by the following elements:

- separateness, within each process, between the subject who initiates it (decision-making impulse), the subject who carries it out and concludes it and the subject who controls it;
- written traceability of each relevant step of the process;
- adequacy of the level of formalization.

To this end, the CA Auto Bank Group has adopted the*SOD Group Policy*, according to which all Group companies must ensure compliance with the principle*"the segregation of duties".*This principle implies the correct separation of roles and responsibilities at all stages of a process, in order to mitigate the risk of errors and/or fraud.

Furthermore, the Bank has also adopted specific Internal Regulations that govern the roles and responsibilities of the various corporate bodies and functions, including internal board committees, joint venture committees, and internal committees.

CA Auto Bank's internal control system is structured in accordance with the Supervisory Provisions for Banks issued by the Bank of Italy. Specifically:

- line controls (so-called "first level controls"), aimed at ensuring that operations are carried out correctly.

- Risk and compliance controls (so-called "second-level controls"), performed respectively by the Risk & Permanent Control and Compliance, Supervisory Relations & Data Protection functions, which aim to ensure, among other things: a. the correct implementation of the risk management process; b. compliance with the operating limits assigned to the various functions; c. compliance of company operations with regulations, including self-regulation.
- internal audit (so-called "third-level controls"), aimed at identifying violations of procedures and regulations as well as periodically assessing the completeness, adequacy, functionality (in terms of efficiency and effectiveness) and reliability of the internal control system and the information system (ICT audit), with a pre-established frequency in relation to the nature and intensity of the risks.

In accordance with Legislative Decree 231/2007, the Bank has established an Anti-Money Laundering Function, entrusted to the Compliance, Supervisory Relations & Data Protection Function, which is responsible for preventing and combating violations of anti-money laundering and countering the financing of terrorism regulations.

1.2 The system of delegations and powers of attorney

Delegation is the internal assignment of functions and tasks, reflected in the organizational communications system. The essential requirements of the delegation system, for the effective prevention of crime, are the following:

- It is the responsibility of the Head of Function/Entity to ensure that all collaborators, who represent the Company even informally, have a written proxy;
- the delegation must indicate:
- delegator (subject to whom the delegate reports hierarchically);
- name and duties of the delegate, consistent with the position held by the same;
- scope of the delegation (e.g. project, duration, product, etc.);
- issue date;
- signature of the delegator.

The system of delegations gives rise to the structure of powers of representation towards third parties, consisting of the set of powers of attorney that the company grants to its employees or third parties, on a special or general and continuous basis, which provide for the definition of financial limits on their exercise for some of the powers granted.

The system of powers of attorney, however, is not perfectly homogeneous with that of delegation, as it differs from the latter in terms of purpose (the decision-making system derives from the delegation system, while the system of powers of attorney provides the set of those who, following decisions made, can bind the company to third parties) and pervasiveness (the system of delegation is a widespread system, while the system of powers of attorney is a targeted system).

In defining its set of powers of attorney, the company adopts prudent criteria aimed at limiting the risk of abuse or incorrect use of the assigned powers, which are also subject to disciplinary action.

The Board of Directors is expressly empowered to approve:

a) of the powers attributed to the Chief Executive Officer and General Manager;
b) of the powers attributed to those directly reporting to the Chief Executive Officer, upon proposal of the latter.

In addition to the Board of Directors, which by law and the bylaws can assign powers to its members, possibly with the right to sub-delegate, the Chief Executive Officer and the Chief Financial Officer can also assign powers, and therefore issue proxies, within the exclusive scope of their assigned powers.

Powers of attorney can be general and valid for continuous exercise, in which case they are issued until revoked, or special, and as such can be exercised in a single context. The latter are issued for specific purposes, generally for the execution of specific acts or contracts.

General powers of attorney are generally issued with a certified signature or through a deed of attorney, and are registered and then entered in the company register, ensuring their publicity towards third parties and thus making them enforceable.

Special powers of attorney may be authenticated or not authenticated, depending on the form of the deed or contract for the execution of which they are produced, or in certain cases on the requirements set by law.

Generally, general powers of attorney are issued to Company employees or employees of other companies seconded to the Company. Powers of attorney to other third parties, whether natural or legal persons, must be limited in the number and nature of their powers, particularly with respect to the procurement of certain professional services or the performance of specific tasks in the name and on behalf of the company.

Maintenance of the power of attorney system (issuing new powers of attorney, modifying existing ones, revoking powers of attorney) is defined by a specific procedure and coordinated by the Company Secretariat.

1.3 Relationships with Customers, Service Companies, Suppliers, Consultants and Partners: general principles of conduct

Relationships with*Customers, Service Companies, Suppliers, Consultants and Partners*, within the scope of Sensitive and Instrumental Processes, must be characterised by maximum correctness and transparency, compliance with the law, the Code of Conduct, this Model and internal company procedures, as well as the specific ethical principles on which the Company's activity is based.

Service Companies, Consultants, Suppliers of products/services and, in general,*Partner*(e.g. temporary business association) must be selected according to the following principles which take into account the elements specified below:

- check the commercial **and professional reliability**(e.g. through ordinary inspections at the Chamber of Commerce to ascertain the consistency of the activity carried out

with the services requested by the Company, self-certification pursuant to Presidential Decree 445/00 relating to any pending charges or sentences issued against them);

- select based on the ability to offer in terms of quality, innovation, costs and sustainability **standards**, with particular reference to respect for human rights and workers' rights, the environment, and the principles of legality, transparency, and fairness in business (this accreditation process must include high quality standards, which can also be verified through the acquisition of specific quality certifications by the organization itself);
- avoid any commercial and/or financial transaction, either directly or through a third party, with individuals or legal entities whose names are involved in investigations by judicial authorities for crimes giving rise to liability pursuant to Legislative Decree 231/01 and/or reported by European and international organizations/authorities responsible for preventing terrorism, money laundering, and organized crime;
- avoid/not accept contractual relationships with subjects - natural persons or legal persons - who have their headquarters or residence or any connection with countries considered non-cooperative as they do not comply with the standards of international laws and the recommendations expressed by the FATF-GAFI (Financial Action Task Force against money laundering) or who are included in the prescription lists (so-called "*Black List*") of the World Bank and the European Commission;
- award compensation exclusively in the event of suitable justification in the context of the contractual relationship established or in relation to the type of assignment to be carried out and current local practices;
- Generally, no payments can be made in cash, and in the event of an exception, such payments must be appropriately authorized. In any case, payments must be made within the scope of specific administrative procedures, which document the traceability and traceability of the expense;
- With regard to financial management, the Company implements specific procedural controls and pays particular attention to flows that fall outside of the company's typical processes and are therefore managed extemporaneously and at discretion. These controls (e.g., frequent reconciliation of accounting data, supervision, segregation of duties, separation of functions, particularly purchasing and finance, effective documentation of the decision-making process, etc.) are intended to prevent the formation of hidden reserves.

1.4 Relationships with Suppliers/Service Companies/Consultants/Partners: Contractual Clauses

Contracts with Suppliers, Service Companies/Consultants/Partners must include specific clauses specifying:

- the commitment to respect the Code of Conduct and the Model adopted by CA Auto Bank, as well as the declaration of never having been implicated in legal proceedings relating to the crimes contemplated in the Company's Model itself and in Legislative

Decree 231/01 (or if they have been, they must in any case declare it for the purposes of greater attention by the Company in the event that the consultancy relationship is established or partnership). This commitment may be reciprocal, in the event that the other party has adopted its own similar code of conduct and Model;

- the consequences of violating the rules set out in the Model and/or the Code of Conduct (e.g. express termination clauses, penalties);
- the commitment, for foreign suppliers/service companies/consultants/partners, to conduct their business in accordance with rules and principles similar to those provided by the laws of the State (or States) where they operate, with particular reference to the crimes of corruption, money laundering and terrorism and to the rules that provide for liability for the legal person (*Corporate Liability*), as well as the principles contained in the Code of Conduct, aimed at ensuring compliance with adequate levels of ethics in the exercise of their activities;
- in the case of procurement, work, or supply contracts, the interested company declares that it employs only personnel hired under a regular employment contract, in full compliance with current legislation on social security, tax, insurance, and immigration regulations;
- that the interested company declares that it has the authorisations required by law to carry out its business;
- that the untruthfulness of the aforementioned declarations could constitute grounds for termination of the contract pursuant to art. 1456 of the Italian Civil Code.

1.5 Relationships with Customers: General Principles of Behavior

Relationships with customers must be characterized by maximum fairness and transparency, in compliance with the Code of Conduct, this Model, legal provisions, and internal company procedures, which take into account, among others, the elements specified below:

- information provided to customers through any channel must be clear, not misleading and compliant with regulatory provisions;
- the credit agreement can only be concluded in the event of proven solvency, on the basis of sufficient information obtained in an appropriate manner;
- contracts must contain all the elements required by applicable legislation, as well as the customer's right to withdraw or terminate the relationship early without having to provide any justification;
- customers must receive periodic communications containing clear and complete information on the progress of the relationship as well as an updated situation of the economic conditions applied;
- Prompt reimbursement of any undue payments made for any reason during the contractual relationship is guaranteed.

1.6 Financial flow management system

The Company, in accordance with the requirements of the relevant Guidelines, adopts a financial flow management system based on principles of transparency, verifiability, and relevance to the company's business. It uses procedural decision-making mechanisms that allow for the documentation and verification of the various stages of the decision-making process, in order to prevent the improper management of the entity's resources.

Proper process management, also in accordance with the provisions of Article 6, paragraph 2, letter c) of Legislative Decree 231/01, helps prevent the risk of the Company committing multiple crimes.

With regard to the management of financial flows, the Company applies the following principles: check:

- separation of duties in key process phases/activities (e.g. authorization, reconciliation);
- system of delegations and powers of attorney constantly aligned with the authorization profiles resident in the information systems;
- system of internal practices/procedures that regulate the main processes impacted by financial flows;
- adequate traceability of information and document flows.

In particular, the Company has adopted practices/procedures that regulate activities related to the management of financial flows, with specific reference to the Rules and Procedures relating to the financial statements as a whole, as well as to the authorization and evaluation of investment initiatives. Furthermore, it avails itself of the indirect Tax Compliance control of the Finance - Tax function to manage the risk of non-compliance with tax regulations.

2. CA Auto Bank's Sensitive/Instrumental Processes

From the risk analysis conducted by CA Auto Bank for the purposes of Legislative Decree 231/01, it emerged that the Sensitive/Instrumental Processes currently mainly concern:

1) Crimes against the Public Administration and Crimes of inducing others not to make statements or to make false statements to the Judicial Authority;
2) Crimes against the individual personality;
3) Crimes of counterfeiting of coins, public credit cards, stamps and instruments or signs of recognition and crimes against industry and commerce
4) Organized crime crimes;
5) Corporate Crimes (including corruption crimes between private individuals);
6) Market Abuse Crimes;
7) Crimes relating to non-cash payment instruments;
8) Crimes of receiving stolen goods, money laundering and use of money, goods or utilities of illicit origin, as well as self-laundering;
9) Crimes aimed at terrorism or subversion of the democratic order;

10) Crimes relating to illegal immigration;
11) Crimes relating to copyright infringement;
12) Computer crimes and unlawful data processing;
13) Crimes of manslaughter and serious or very serious bodily harm committed in violation of accident prevention and workplace health and hygiene regulations;
14) Environmental crimes;
15) Transnational crimes;
16) Tax crimes

The risk relating to the other types of crimes contemplated by Legislative Decree 231/01 appears only abstract and not concretely conceivable.

The details of the criminal offences listed above are reported in Appendix A.

The aim of this Section is to:

- represent, for each family of Crimes applicable to the Company, the Company Functions / Departments involved and the internal processes of CA Auto Bank included in the Sensitive and Instrumental Processes identified in this Model;
- indicate the principles, obligations and prohibitions that the Recipients – see Section II, paragraph 1.4 – are required to observe for the purposes of effectively preventing the risk of committing crimes when carrying out activities in which the risk of committing one of the crimes mentioned above is conceivable;
- provide the Supervisory Body and the heads of other corporate functions that cooperate with it with the executive tools to carry out control, monitoring and verification activities through the procedures in force and in the process of being issued by the Company.

2.1 Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in articles 24, 25, and 25-*ten times of* Legislative Decree 231/01 are the following:

- Customer Relationship Management; (Annex C, sheet 14)
- Management of activities/remarketing; (Annex C, sheet 06)
- Management of administrative obligations, relations with Supervisory Authorities, and related inspection activities; (Annex C, sheet 18)
- Management of litigation and relations with the Judicial Authority and management of settlement agreements; (Annex C, sheet 12)
- Management of development activities; (Annex C, sheet 05)

In relation to the crimes discussed in this Section, the Company has also identified the following Instrumental Processes:

- Management of purchases of goods and services (including consultancy); (Annex C, sheet 19)
- Selection and management of *partner* commercial. (Annex C, sheet 02)
- Personnel Management and Reward System; (Annex C, Sheet 11)
- Management of expense reports and entertainment expenses; (Annex C, sheet 04)
- Financial Flow Management; (Annex C, Sheet 15)
- Management and assessment of customer credit; (Annex C, sheet 03)
- Relationship Management intercompany; (Annex C, sheet 01)
- Management of gifts, donations, events, and sponsorships; (Annex C, sheet 16)
- Management of internal and external communications (investors, advertising, etc.); (Annex C, sheet 09)

The Corporate Functions/Departments involved in the Sensitive and Instrumental Processes listed above and falling within the specific Crime Family are identified in Annex C to this Model. Annex C also contains the internal processes and related corporate procedures.

The general criteria for the definition of Public Administration and, in particular, of Public Official and Public Service Representative, are reported in Annex A.

This definition includes a broad category of entities with which the Company may operate in the performance of its business, as it includes, in addition to Public Bodies and those performing a public legislative, judicial, or administrative function (Public Officials), also those entities/entities entrusted by the Public Administration—for example, through an agreement and/or concession and regardless of the legal nature of the entity/entity, which may also be under private law—with the care of public interests or the satisfaction of needs of general interest (public service representatives).

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory to** ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in Articles 24, 25, 25-*to have* (as specified above) and 25-*ten times of* Legislative Decree 231/2001 referred to above.

***

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Customer relationship management;*
- *Management of remarketing activities;*

Customer relationship management and management of business activities*remarketing*could present risk profiles in relation to crimes against the Public Administration in the event that a subordinate or senior member of the Company:

- offers or promises money or other benefits to a public official, a person in charge of a public service or to persons indicated by them
- misleads a public official through artifice or deception (such as, for example, the falsification or alteration of documents prepared for the Public Administration) in order to acquire the relevant Public Administration as a client.

To the Recipients as defined above who, by reason of their role or function, are involved in the management of the aforementioned activities it **is mandatory** Of:

- ensure, where necessary, that customer relationships are managed exclusively by persons with appropriate powers;
- ensure that relationships with public administration officials or public service representatives are managed exclusively by individuals with appropriate powers, previously identified and authorized by the Company;
- in the event of requests for donations of money or valuable goods by a public official, the interested party has the obligation to refuse any payment, even if subjected to illicit pressure, and to promptly inform the Supervisory Body;
- in the event of conflicts of interest that arise in the context of relations with the Public Administration, the interested party must promptly inform the Supervisory Body;
- ensure compliance with all provisions of the Group's policies and procedures, particularly those relating to anti-money laundering, antitrust and conflict of interest;
- ensure the traceability of all phases of the commercial process, including the definition of financial conditions, any discounts applied, and the duration of agreements, through the use of the required information systems;
- provide for adequate segregation of tasks and responsibilities in customer management, with particular reference to the definition of financial conditions and payment methods and times;
- ensure that commercial offers/proposals are defined on the basis of company procedures;

- ensure that relationships with customers are formalized in specific written agreements (e.g. commercial offers/proposals), approved by persons with specific powers;
- ensure that preliminary screening is carried out on new clients, both in terms of compliance, including anti-money laundering, and creditworthiness;
- Ensure the segregation of duties throughout all phases of customer relationship management and remarketing activities, including the creation of customer records. Ensure that any exceptions to the financial conditions, determined automatically through a dedicated system, are authorized in accordance with the provisions of the system of delegations and powers of attorney;
- ensure the traceability of all phases of the sales entity agreement process;
- carry out specific verification activities related to credit management;
- ensure the traceability of all documentation sent to customers;
- verify the regularity of invoicing towards customers;
- carry out a specific analysis of complaints received from customers;
- forward the financing application to the competent signature level for the approval;
- in the event that the services provided to customers are carried out - in whole or in part - with the support of third parties, ensure that their selection always takes place in compliance with the provisions set out in the "Selection and Management of Commercial Partners" section of this chapter;
- ensure the monitoring of the credit positions of customers who hold the position of public officials or persons in charge of a public service;
- promptly communicate to their immediate superior or to the Company's management and, at the same time, to the Supervisory Body any conduct by those working for the counterparty aimed at obtaining favors, illicit donations of money or other benefits, including from third parties, as well as any critical issues or conflicts of interest that arise within the scope of the relationship.

In the context of the aforementioned behaviors. **it is forbidden** Of:

- making promises or undue donations of money or other benefits (for example: hiring, assigning professional, commercial or technical positions) to public officials, public service employees, private individuals or people close to them;
- make services or payments to third parties operating on behalf of the Company in the context of the activities governed by this chapter, which are not adequately justified in the context of the contractual relationship established with them;
- submit offers that have not been subjected to the approval process required by company procedures;
- enter into contracts with conditions established according to non-objective parameters and/or in violation of the provisions of company procedures and relevant legislation;

- submitting untrue statements by presenting documents that do not correspond in whole or in part to reality or by omitting to present real documents;
- engage in misleading conduct towards the Public Administration;
- be represented in relations with the Public Administration by consultants or third parties who could create conflicts of interest; solicit and/or obtain confidential information that could compromise the integrity or reputation of either party;
- influence, during any business negotiation, request or relationship with the Public Administration, the decisions of officials who deal with or make decisions on behalf of the PA;
- granting credit outside the circumstances contemplated by company credit policies with the aim of obtaining an undue advantage for a customer who also holds the status of a public official or person in charge of a public service.

***

The main examples of crimes with reference to the following Sensitive Process are listed below:

- *Management of administrative obligations, relations with Supervisory Authorities, and related inspection activities.*

Managing relationships with the Public Administration for the issuance of certifications, authorizations, or permits could present risks related to the crime of fraud against the State in the event that, for example, a senior executive or subordinate of the Company misleads the Public Administration not simply by submitting false declarations or documents or certifying untrue circumstances, but also by engaging in further deceit, such as attaching invoices for non-existent transactions, in order to unduly obtain, for themselves or others, an authorization or permit granted by the Public Administration.

Managing relationships with public officials in the event of audits and inspections by Supervisory Authorities or Public Administration agencies (Financial Police, Local Health Authority, Regional Environmental Protection Agency, etc.) could present risks related to the crime of corruption for committing an act contrary to official duties, for example, if a senior executive or subordinate of the Company delivers or promises money or other benefits to a public entity in order to induce them to successfully complete the audit.

Managing relationships with the Public Administration could present risks related to the crime of illicit influence peddling if, for example, a senior executive or subordinate of the Company offers or promises money or other benefits to a third party who claims to have actual relationships with a public official or public service representative, so that the third party may act as an intermediary in relations with the Public Administration to obtain preferential treatment or undue advantages for the Company, such as, for example, the issuance of certifications, authorizations, or permits or the successful completion of an audit.

To the Recipients as defined above who, by reason of their role or function, are involved in the management of the aforementioned activity it **is mandatory** Of:

- ensure compliance with all provisions of the *policy and* Group procedures, particularly those relating to *antitrust and* conflict of interest;
- ensure that relationships with Public Administration officials are managed exclusively by individuals with appropriate powers, previously identified and authorized by the Company, as required by internal procedures;
- identify the resources responsible for managing relations with the Supervisory Authorities during inspection visits;
- in the event of inspection visits, ensure that at least two Company resources participate in the meetings;
- ensure the signing of the minutes/*summaries* by a company person authorised to do so or by those who witnessed the inspection operations;
- ensure the traceability of relationships with the Public Administration;
- periodically monitor the deadlines for sending data and mandatory communications to the competent Authority;
- promptly and correctly, truthfully and completely, carry out the communications required by the Law, regulations and company rules in force from time to time towards the Authorities or supervisory or control bodies;
- ensure that the Authority receiving the communications has received the communication (obtain a response from the public body or keep a copy of the return receipt if the correspondence is sent by registered mail with return receipt);
- comply with the authorization process imposed by the delegation system and internal operating provisions;
- promptly transmit periodic reports to the Supervisory Authorities and promptly respond to requests/requests received from the same Authorities;
- establish relationships with the Authorities based on maximum transparency, collaboration, availability, and full respect for their institutional role, avoiding any conduct that hinders the exercise of supervisory functions (for example, express opposition, unjustified refusals, delays in transmitting or delivering documents, etc.);
- promptly implement the provisions of the same Authorities;
- carry out obligations towards the Authorities with the utmost diligence and professionalism, in order to provide clear, accurate, complete, truthful, and truthful information, so as to avoid conflicts of interest and in any case provide timely information and in the manner deemed most appropriate;
- transmit the signed minutes containing provisions, sanctions, observations, etc. to the Chief Executive Officer and the Supervisory Body;
- in the event that the documentation to be sent to the Public Administration is produced - in whole or in part - with the support of third parties (consultants, lawyers, etc.), ensure that the selection of the same always takes place in compliance with the provisions set out

in the section "*Management of purchases of goods and services (including consultancy)*" of this chapter;

- ensure that access to the IT/telematic systems of Public Administrations is carried out exclusively by authorised personnel equipped with appropriate *password* staff;
- ensure that checks are carried out to prevent the spread of password to enable unauthorized persons to access the public administration's IT/telematic systems;
- communicate, without delay, to your hierarchical manager or to the *management of* the Company and, together with the Supervisory Body, any conduct carried out by those who operate with the public counterpart, aimed at obtaining favors, illicit donations of money or other benefits, including towards third parties, as well as any critical issues or conflicts of interest that arise within the context of the relationship with the Public Administration;
- transmit to the Supervisory Body, on a six-monthly basis, the list of delegations and powers of attorney issued to company representatives for the purpose of maintaining relations with the Public Administration;
- promptly report to the Supervisory Body any inspections received and/or in progress, specifying: (i) the Public Administration carrying out the inspection; (ii) the participating entities; (iii) the object of the inspection and (iv) the period during which it was carried out.

In the context of the aforementioned behaviour it **is forbidden** Of:

- maintain relationships with Public Administration Officials or public officials without the presence of at least one other person, where possible, and without ensuring traceability, as specified above;
- make promises or undue donations of money or other benefits (for example: gifts of significant value, hiring, assignments of professional, commercial or technical roles) to public officials or public service representatives or persons close to them or to private individuals, with the aim of promoting or favoring the interests of the Company;
- engage in behavior intended to improperly influence the decisions of officials who deal with or make decisions on behalf of the Public Administration; give in to recommendations or pressure from public officials or public service representatives;
- submitting untrue statements by presenting documents that do not correspond in whole or in part to reality or by omitting to present real documents;
- engage in misleading conduct towards the Public Administration such as to induce the latter to make errors of judgment during the analysis of requests for authorizations and similar;
- be represented in relations with the Public Administration by consultants or third parties who may create conflicts of interest.

***

The main examples of crimes with reference to the following Sensitive Process are listed below:

• *Litigation management and relations with the Judicial Authorities and management of settlement agreements.*

The management of litigation and relations with the Judicial Authority could present risks related to the crime of corruption in judicial proceedings (either directly or through legal advisors) in the event that a senior manager or subordinate of the Company, in order to favor the latter in a civil, criminal, or administrative proceeding involving it, offers money to the appointed magistrate.

Managing relationships with the Judicial Authority may present risks related to the crime of inducement and refusal to make statements or to make false statements to the Judicial Authority in the event that, for example, a senior executive or subordinate of the Company accused or under investigation in a criminal proceeding is induced to make false statements (or to refrain from making them) to avoid the Company being held liable.

With reference to the activity envisaged above, the specific principles of conduct are indicated below.

To the Recipients as defined above who, by reason of their role or function, are involved in the management of the aforementioned activity it **is mandatory** Of:

- ensure, in interactions with public counterparts, compliance with the provisions of internal procedures;
- identify a person responsible, consistent with the subject matter, with the necessary powers to represent the company or to coordinate the actions of any external professionals;
- ensure that relations with the Public Administration are maintained by subjects previously identified and authorised by the Company;
- periodically monitor ongoing legal proceedings;
- in the event that the activity is managed - in whole or in part - with the support of third parties (consultants, lawyers, etc.), ensure that the selection and qualification of the same always takes place in compliance with the provisions set out in the section "Management of purchases of goods and services (including consultancy)" of this chapter;
- assign the task to external professionals through the stipulation of specific written contracts, indicating the agreed-upon compensation and the content of the service, and authorised by personnel with appropriate powers;
- ensure that the roles and responsibilities of the individuals responsible for managing the conclusion of settlement agreements are clearly identified;
- ensure transparency and traceability of inter negotiations aimed at concluding settlement agreements;
- observe the rules governing the evaluation criteria and the authorization process for settlement agreements.

In carrying out all operations relating to the management of relations with the Judicial Authority, in addition to the set of rules set out in this Model, the Recipients **is mandatory to** know and respect the following:

- in relations with the Judicial Authority, the Recipients are required to provide active cooperation and to make truthful, transparent and exhaustively representative declarations of the facts;
- in relations with the Judicial Authority, the Recipients and, in particular, those who may be under investigation or accused in criminal proceedings, including related proceedings, relating to their work within the Company, are required to freely express their representations of the facts or to exercise the right to remain silent granted by law;
- All Recipients must promptly notify the Supervisory Body, through the communication tools existing within the Company (or with any communication tool, provided that the traceability principle is respected), of any act, summons to testify and legal proceedings (civil, criminal or administrative) that involve them, in any respect, in relation to the work activity performed or in any way related to it;
- The Supervisory Body must be able to obtain full knowledge of the ongoing proceedings, including through participation in meetings relating to the relevant proceedings or in any case preparatory to the defensive activity of the Recipient, even in cases where the aforementioned meetings involve the participation of external consultants.

To the Recipients as defined above who, by reason of their role or function, are involved in the management of litigation and relations with the Judicial Authority and in the management of settlement agreements it **is forbidden** Of:

- make services or payments to external lawyers, consultants, experts, or other third parties operating on behalf of the Company, which are not adequately justified in the context of the contractual relationship established with them;
- adopt behaviors contrary to the laws and the Code of Conduct during formal and informal meetings, including through external lawyers and consultants, to induce Judges or Members of Arbitration Panels (including assistants and court-appointed experts) to unduly favor the interests of the Company;
- adopt behaviors contrary to the laws and the Code of Conduct during inspections/controls/audits by public bodies or official experts, to influence their judgment/opinion in the interests of the Company, including through external lawyers and consultants;
- coerce or induce, in any form and by any means, in the misconceived interest of the Company, the will of the Recipients to respond to the Judicial Authority or to avail themselves of the right not to respond;
- accept, in relations with the judicial authorities, money or other benefits, even through consultants of the Company itself;
- induce the Recipient, in relations with the Judicial Authority, to make untrue statements.

***

The main examples of crimes with reference to the following Sensitive Process are listed below:

• *Management of development activities.*

The management of new service development activities could present risks related to crimes against the Public Administration and its assets if, for example, the Company were to prepare a new contractual model aimed at public clients containing misleading information aimed at inducing the Public Administration to enter into the contract.

To the Recipients as defined above who, by reason of their role or function, are involved in the management of the aforementioned activity it **is mandatory**Of:

- ensure compliance with both local and Group operating procedures;
- ensure compliance with the rules of segregation of duties between the person who prepares the*New Product and Activities (NPA) Concept*, who carries out the evaluation and who carries out the related control;
- carry out a specific analysis of the risks associated with new products and new activities, in compliance with the law and regulatory developments;
- ensure that documentation is archived at the functions involved in the process;
- ensure that all new services developed are approved by entities with appropriate powers;
- ensure traceability of all stages of the process.

In the context of the aforementioned behaviour it **is forbidden** Of:

- engage in behaviors intended to improperly influence the decisions of officials who deal with or make decisions on behalf of the Public Administration;
- submitting untrue statements by presenting documents that do not correspond in whole or in part to reality or by omitting to present real documents;
- engage in misleading conduct towards the Public Administration that may lead the latter to make errors of assessment when analyzing the characteristics of the services offered.

***

The main examples of crimes with reference to the following Instrumental Process are listed below:

• *Management of purchases of goods and services (including consultancy).*

The management of procurement of goods and services (including consultancy) could present risks related to the configuration of crimes against the Public Administration if the identification of a specific supplier occurs following a recommendation from a Public Administration official as the price of a corrupt agreement.

The management of purchases of goods and services (including consultancy) could present risks related to the crime of illicit influence peddling if, for example, a senior executive or subordinate of the Company offers or promises money or other benefits to a consultant who, taking advantage of the consultant's relationships with a public official or public service representative, may act as an intermediary in relations with the Public Administration to obtain

preferential treatment or undue advantages for the Company, such as, for example, the issuance of certifications, authorisations or permits or the successful outcome of an audit.

With reference to the activity envisaged above, the specific principles of conduct are indicated below.

In managing relationships with suppliers of goods and services, the Company must introduce specific contractual clauses into purchase orders/contracts as set out in paragraph *"Relationships with Suppliers/Service Companies/Consultants/Partners: Contractual Clauses"*To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of purchases of goods and services (including consultancy) **it is mandatory** Of:

- create a specific supplier registry, in order to collect and record all critical and significant information about them;
- avoid conflicts of interest, particularly with regard to personal, financial, or family interests (e.g., financial or commercial interests in supplier companies, customers, or competitors, improper advantages arising from one's role within the Company, etc.), which could affect independence from suppliers;
- subject suppliers to a qualification process that allows for the verification of their financial soundness, commercial, technical-professional and ethical reliability;
- ensure that the selection of suppliers and consultants takes place among the names selected on the basis of criteria identified within the internal regulations, without prejudice to occasional needs/supplies
- ensure compliance with the *iter* approval of suppliers and contracts, as required by company procedures;
- ensure adequate segregation of functions in the supplier/consultant selection process;

  proceed, in accordance with company procedures, to select the supplier by comparing three offers, except in special cases which must be duly justified (such as: low-value contracts, intra-group agreements, contracts with specific companies, a relationship of trust established with the consultant or supplier, etc.);
- verify the existence of specific authorizations of suppliers who carry out activities for which they are required;
- verify, during the qualification phase and periodically, the possible presence of Suppliers in the *Black List*;
- ensure traceability, including through specific information systems, of their supplier selection, qualification and evaluation, through the formalization and archiving of the relevant supporting documentation, in the manner established by company procedures and the IT tools supporting the process;
- ensure that all payments to suppliers are made if adequately supported by contract or order, only following validation according to their predefined internal authorization and after having verified the compliance of the products with what was ordered;

- verify the regularity of payments to suppliers, with reference to the full correspondence between recipients/orderers and the counterparties actually involved;
- ensure that all relationships with suppliers or consultants are formalized within specific written agreements approved according to the delegation system and where the price of the goods or the consideration for the service is clearly defined;
- ensure that contracts stipulated with suppliers/consultants specifically provide for: object of the contract, agreed compensation, payment method, ethical and contractual clauses, compliance, termination clauses or alternatively verify that the contractual conditions proposed by third parties provide for compliance with the principles set out in Legislative Decree 231/01, as well as ethical ones;
- ensure the traceability and retrospective reconstructability of commercial transactions through the formalization and archiving, including through specific information systems, of the relevant supporting documentation;
- ensure periodic monitoring, through the use of specific tools, of the suppliers' performance, as well as use the results of these assessments for the purposes of their qualification;
- In the case of outsourced services that require the use of non-EU personnel, verify the validity of the relevant residence permits;
- carefully investigate and report to the Supervisory Body:
  the requests for unusually high fees; or requests for expense reimbursements that are not adequately documented or are unusual for the operation in question.

In the context of the aforementioned behaviour it **is forbidden** Of:

- make payments in cash, to numbered current accounts or accounts not in the name of the supplier or other than those provided for in the contract;
- make payments in countries other than the supplier's country of residence;
- making payments that are not properly documented;
- create funds against unjustified payments (in whole or in part);
- bind the Company with verbal orders/contracts with consultants;
- carry out any commercial or financial transaction, either directly or through a third party, with entities (natural or legal persons) whose names are included in the Lists available at the Bank of Italy, or by entities controlled by the latter, when such control relationship is known;

  Providing services to consultants and suppliers that are not adequately justified within the contractual relationship established with them, and paying them compensation that is not adequately justified in relation to the type of assignment to be performed and current local practices.

***

The main examples of crimes with reference to the following Instrumental Process are listed below:

- *Selection and management of commercial partners.*

The selection and management of partner/commercial activities could present risk profiles in relation to crimes of corruption of representatives of the Public Administration in the event that, for example, a subordinate or senior individual of the Company stipulates fictitious contracts or contracts with values that are deliberately not in line with partners in order to create funds to be used for corrupt purposes.

With reference to the selection and management process of *partner* commercial, the specific principles of behavior are indicated below.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the aforementioned activity it **is mandatory** Of:

- avoid conflicts of interest, particularly with regard to personal, financial, or family interests (e.g., financial or commercial interests in supplier companies, customers, or competitors, improper advantages arising from one's role within the Company, etc.), which could influence independence from partners;
- ensure that the selection and qualification process of partner/commercial transactions always take place in full compliance with the provisions of company procedures*;*
- ensure an adequate process of *due diligence* of any *partner* commercial which includes, among other things, the verification of the commercial and professional reliability and the integrity requirements of the counterparties;
- verify, during the qualification phase and periodically, the possible presence of partner in the *Black List*;
- verify the identity of the counterparty;
- ensure the traceability of the *iter* of selection;
- respect the principles of transparency, professionalism, reliability, motivation and non-discrimination in the choice of the counterparty;
- ensure that the agreed fees fall within normal market conditions and are in any case contractually defined on the basis of objective calculation criteria;
- ensure that the contractual mechanism used contains specific information on the rules of conduct adopted by the Company with reference to Legislative Decree 231/2001 and on the consequences that behaviors contrary to the provisions of the Code of Conduct and current legislation may have with regard to contractual relationships;
- ensure that the assignment of the mandate to the counterparty is evidenced by a written document;

  Disburse fees transparently, always documentable, and reconstructable after the fact. In particular, verify the correspondence between the recipient of the payment and the provider of the service;
- submit the *partner* qualified for checks and *audit* periodicals as required by company procedures;

- ensure that incentives and bonus, in cash or in kind, are paid upon achievement of predetermined company objectives;
- communicate promptly to your hierarchical manager or to the *management of* the Company and, at the same time, to the Supervisory Body, also through the communication tools existing within the Company, any suspicious behavior or activities carried out by those working for the counterparty.

In the context of the aforementioned behaviors **it is forbidden** Of:

- bind the Company with verbal contracts with the counterparty;
- issue or accept invoices for non-existent transactions;
- make payments and reimburse expenses to counterparties that are not adequately justified in relation to the type of business performed, are not supported by fiscally valid receipts, and are not shown on the invoice;
- certify the receipt of non-existent commercial services;
- create extra-accounting equity funds for transactions contracted at above-market conditions or for invoices that are non-existent in whole or in part.

***

The main examples of crimes with reference to the following Instrumental Process are listed below:

- *Personnel management and reward system.*

Personnel management could present risks related to the crime of corruption if, for example, a candidate close to or recommended by a public official is chosen in order to obtain an undue advantage for the Company.

Management of the reward system could pose risks related to corruption, should the Company provide a resource with cash bonuses/incentives that are intentionally disproportionate to their role/skills, in order to provide the employee with funds to engage in corrupt practices. With reference to the above-mentioned activity, the specific principles of conduct are outlined below.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the selection and management of personnel it **is mandatory** Of:

- ensure that the processes identified above always take place in compliance with the provisions of company procedures;- operate in compliance with the criteria of:
  a) meritocracy, evaluating curricular professional skills;
  b) respect for the real needs of the Company;
  c) personal dignity and equal opportunities;
- carry out selection activities aimed at ensuring that the choice of candidates is made on the basis of objective considerations of the professional and personal characteristics necessary to carry out the work to be performed, avoiding favoritism of any kind;

- ensure the segregation of the selection process by ensuring that interviews are conducted by the Human Resources department and the Head of the requesting Function;
- subject candidates to evaluation interviews and, in order to ensure full traceability of the process, formalize the results of each interview in specific documentation whose archiving is guaranteed;
- ensure that the hiring request and the subsequent contract are authorised, verified and signed by the department managers according to the existing system of delegations and powers of attorney;
- operate in compliance with the criterion of meritocracy and equal opportunities, without any discrimination based on gender, racial or ethnic origin, nationality, age, political opinions, religious beliefs, health status, sexual orientation, economic or social conditions, in relation to the real needs of the Company;
- ensure that the candidate is first asked to declare any family relationships with members of the Public Administration and, if so, the possible existence of any potential conflict of interest is assessed;
- ensure that the existence of possible conflicts of interest and any potential conflicts of interest are verified status of a former public employee of the candidate, in order to ensure compliance with the provisions of Legislative Decree 165/2001, art. 53, paragraph 16-*to have*(introduced by Law 190/2012 on “Anti-corruption”);
- hire staff only and exclusively with a regular employment contract and with remuneration consistent with the applicable Collective Bargaining Agreement;
- ensure that upon hiring, the employee is given a copy of the Code of Conduct and this Model and that he or she formally commits to full compliance with the principles contained therein;
- ensure an adequate training process of *induction to* the new hire which provides, among other things, adequate information regarding the Model and the Company's Code of Conduct;
- ensure the existence of documentation certifying the correct execution of the selection and hiring procedures;

  verify that working hours are applied in compliance with current legislation;
- ensure that working conditions within the Company that respect personal dignity, equal opportunities and a suitable working environment are ensured, in compliance with the collective bargaining agreements of the sector and with social security, tax and insurance regulations;
- ensure that the definition of the economic conditions is consistent with the position held by the candidate and the responsibilities/tasks assigned;
- ensure the archiving of the remuneration surveys periodically conducted by the Company;
- for personnel from non-EU countries, verify the validity of the residence permit and monitor it throughout the duration of the employment relationship;

- where third parties are used for the selection of candidates, ensure that the relationships with the aforementioned parties are formalised through written contracts containing clauses specifying: that the third party declares that it respects the principles set out in Legislative Decree 231/2001, as well as adhering to the principles of the Code of Conduct;
    - o that the third party declares that it has implemented all necessary measures and precautions aimed at preventing the crimes indicated above, having equipped its corporate structure – where possible – with internal procedures and systems that are fully adequate for such prevention;
    - o that the untruthfulness of the aforementioned declarations could constitute grounds for termination of the contract pursuant to art. 1456 of the Italian Civil Code;
- ensure that the contracts are signed by persons with appropriate powers;
- ensure the traceability and archiving of all phases of the personal loan disbursement process for Group employees, their first-degree relatives, and their spouses and relatives;
- ensure that the incentive system is consistent with the Group's remuneration policy
- ensure the segregation of the incentive system, providing for the involvement of the HR function and the relevant company departments;
- set maximum limits on variable compensation, consistent with assigned responsibilities and duties and applicable legislation;
- ensure that any incentive systems correspond to realistic objectives and are consistent with the tasks, activities performed and responsibilities assigned;
- provide for limitations to the incentive system in the event of inappropriate behavior, which is the subject of a formal action by the Company (e.g. the imposition of disciplinary sanctions);
- ensure the traceability of the incentive process, through the formalization of objectives and the related reporting.

In the context of the aforementioned behaviors **it is forbidden** Of:

- operate according to the logic of favoritism;
- tolerate forms of irregular or child labor or exploitation of labor;
- hiring personnel, even on temporary contracts, without complying with current regulations (for example, regarding social security and welfare contributions, residence permits, etc.);
- hire or promise to hire Public Administration employees (or their relatives, in-laws, friends, etc.) who have participated in Public Administration authorization processes or inspections of the Company;
- promising or granting promises of hiring/career advancement to resources close to or favored by public officials when this does not comply with the company's real needs and does not respect the principle of meritocracy.

***

The main examples of crimes with reference to the following Instrumental Process are listed below:

• *Management of expense reports and entertainment expenses.*

The management of expense reports could present risks related to crimes against the Public Administration, in the event that the Company, in order to provide employees with supplies to be used for corrupt purposes, reimbursed fictitious expenses or expenses not falling within the employee's normal activities.

The management of entertainment expenses could present risks related to corruption crimes, for example, if a senior executive or subordinate of the Company were to use sums subsequently accounted for as entertainment expenses to bribe a public official.

With reference to the activities envisaged above, the specific principles of conduct are indicated below.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of expense reports and entertainment expenses **it is mandatory** Of:

- prepare expense reports in compliance with company procedures, using dedicated company IT tools;
- ensure that expense claims are reimbursed only after approval by appropriately authorized persons, based on a segregated process, and only in the presence of proper supporting documents;
- ensure compliance with the rules adopted by the Company regarding corporate credit cards and the types of expenses permitted;
- ensure that company credit cards are assigned to appropriately authorized personnel;
- ensure the presence of supporting documents relating to expenses made with company credit cards;
- carry out specific checks and monitoring regarding the use of company credit cards and, more generally, employee expense reports;
- ensure compliance with the internal limitations defined by company procedures regarding expense reports and the use of company credit cards, as well as regarding entertainment expenses;

  verify that the expenses incurred are related to the performance of the work activity, appropriate and adequately documented by attaching fiscally valid receipts;
- ensure that entertainment expenses are not repetitive for the same beneficiary and that full traceability of the participating entities is guaranteed;
- ensure a periodic verification process of staff expense reports;
- ensure that, in the event of abnormal expenses, they are not reimbursed.

In the context of the aforementioned behaviour it **is forbidden** Of:

- incur expenses for meals, entertainment, or other forms of hospitality outside of those provided for by company procedures; - make expense reimbursements that:

- have not been duly authorized;
- do not find adequate justification in relation to the type of activity carried out;
- are not supported by fiscally valid documents or are not shown in the notes.

***

The main examples of crimes with reference to the following Instrumental Processes are listed below:

- *Financial flow management;*
- *Management and evaluation of customer credit;*
- *Management of intercompany relationships.*

The lack of transparency in the management of financial resources could pose risks related to crimes against the Public Administration, for example, if the Company were allowed to set aside funds for corrupt purposes.

Alternatively, it is possible that the Company could move financial flows to disrupt the progress of a public tender and thus favor one of the participants (which, for example, could be one of its subsidiaries).

The management and assessment of customer credit could present risks related to the crime of corruption if, for example, a subordinate or senior executive of the Company authorizes a write-off of credit, even without the requirements, in order to grant a benefit to the counterparty and create funds to be used for corruption purposes.

Relationship management*intercompany*It could present risk profiles in relation to crimes against the Public Administration and its assets in the event that the Company were to use financial resources in transactions with Group companies in order to create funds to be used for corrupt purposes.

With reference to the activities envisaged above, the specific principles of conduct are indicated below.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of financial flows, in the management and evaluation of customer credit and in the management of intercompany relationships it **is mandatory** Of:

- ensure that the management of financial resources is carried out in accordance with the rules defined by the Company;
- authorize only previously identified individuals with specific power of attorney to manage and move financial flows;
- ensure a payment approval process, in accordance with the Bank's system of delegations and powers of attorney;
- carry out procedural controls with reference to financial management, with particular attention to flows that do not fall within the company's typical processes and which are

therefore managed in an extemporaneous and discretionary manner, in order to prevent the formation of hidden reserves;

- ensure the evaluation and monitoring of investments made;
- ensure that all provisions relating to bank accounts held in the Company's name, as well as payments made using other methods (e.g., company credit cards), are adequately documented and authorised in accordance with the current delegation system;
- monitor bank reconciliations on a monthly basis;
- when using the funds in the petty cash box, comply with internal company rules as well as the limits on the use of cash set out in current legislation;
- establish limits on the autonomous use of financial resources by defining quantitative thresholds consistent with the organizational roles and responsibilities assigned to individuals;
- carry out all financial flow movements with tools that guarantee their traceability;
- ensure that, for the management of incoming and outgoing flows, only the channels of banks and other accredited financial intermediaries subject to European Union regulations or credit/financial institutions located in a non-EU country are used, which impose obligations equivalent to those required by anti-money laundering laws and provide for the monitoring of compliance with such obligations;
- ensure adequate segregation between those who can upload payment slips, the approvers, and those who manage sensitive data within supplier databases;
- ensure that banking operations, such as opening and closing the Company's bank accounts and other dispositive operations, are authorised only by persons with adequate powers;
- ensure that relationships/intercompany are regulated by specific contracts/agreements governing, among other things, roles, responsibilities and agreed compensation;
- ensure the correct and complete preparation, in line with the provisions of applicable legislation, of transfer pricing documentation, suitable for certifying the conformity of the transfer prices applied in intragroup transactions with the "normal value";
- ensure that the above documentation contains, among other things, the following information:
  - mapping of intra-group transactions;
  - the definition of cost-sharing agreements;
  - the formulation of a transfer pricing policy;
- ensure that the documentation is signed by persons with appropriate powers; evaluate credit towards customers through the use of credit management systems*rating;*
- ensure that credits are written off only on the basis of internal policies and procedures, reliable documentation certifying the actual irrecoverability of the credit, and in accordance with accounting principles and tax regulations;

- where third parties are used for credit management, ensure that relationships with the aforementioned parties are formalised through written contracts containing clauses specifying: that the third party declares that it respects the principles set out in Legislative Decree 231/2001, as well as adhering to the principles of the company's Code of Conduct;
    - that the third party declares that it has implemented all necessary measures and precautions aimed at preventing the crimes indicated above, having equipped its corporate structure – where possible – with internal procedures and systems that are fully adequate for such prevention;
    - that the untruthfulness of the aforementioned declarations could constitute grounds for termination of the contract pursuant to art. 1456 of the Italian Civil Code;
- ensure that the selection of any third parties takes place in compliance with the provisions set out in the section "*Management of purchases of goods and services (including consultancy)"*of this chapter;
- ensure that documentation is archived at the functions involved in the process;
- communicate, without delay, to *management* company and, at the same time, the Supervisory Body, any critical issues that may arise within the scope of the activity in question.
- report to the Supervisory Body, on a six-monthly basis, the results of the checks carried out on incoming and outgoing financial flows, indicating any anomalies found (for example, lack of supporting documentation, flows relating to purposes not related to the company's activity, etc.).

In the context of the aforementioned behaviors**it is forbidden** Of:

- make cash payments for amounts exceeding regulatory limits or with untraceable payment methods;
- make payments to numbered current accounts or accounts not in the name of the supplier;
- make payments to current accounts other than those contractually provided for;
- making payments that are not properly documented;
- receive payments from parties who have no commercial/contractual relationship with the Company, except in specific cases governed by company procedures;
- create funds for unjustified payments (in whole or in part), including through relationships with companies belonging to the Group;
- create, or allow to be created, illicit, hidden or otherwise incorrectly accounted funds, through any illicit, simulated, fictitious and/or incorrectly accounted financial operation or movement;
- make transfers of cash or bearer bank or postal deposit books or bearer securities in euros or foreign currency, when the value of the transaction, even if split, is overall equal to or greater than the limit established by the Anti-Money Laundering Regulations;
- make requests for the issuance and use of free-form bank and postal cheque forms, in place of those with a non-transferability clause;

- issue bank and postal checks that do not indicate the name or company name of the beneficiary and do not contain a non-transferability clause;
- open accounts or savings books anonymously or under fictitious names and use those opened in foreign countries;
- make bank transfers without indicating the counterparty;
- make money transfers for which there is no full correspondence between the recipients/payers and the counterparties actually involved in the transactions;
- make payments or recognize compensation in favor of third parties operating on behalf of the Company, which are not adequately justified in the context of the contractual relationship established with them;
- make payments to/from an account other than the one indicated in the account details or relating to credit institutions based in tax havens or which do not have physical establishments in any country;
- make payments to/from counterparties based in tax havens, countries at risk of terrorism, etc.;
- authorize the transfer to loss of credits without the requirements being met;
- enter into relationships with parties attributable to contracting authorities, or with third parties participating in public tenders called by the same contracting authorities, with the aim of unduly interfering in the definition of the tender notice or in the award procedures.

***

The main examples of crimes relating to the following activities are listed below:

- *Management of gifts, donations, events and sponsorships;*
- *abuse (investors, advertising, etc.).*

The management of gifts, donations, events, and sponsorships could pose risks related to corruption if a senior executive or subordinate of the Company grants gifts of significant value to public counterparties in order to commit corrupt acts and obtain illicit benefits.

The management of internal and external communications (investors, advertising, etc.) could present risks related to corruption crimes in the event that a senior executive or subordinate of the Company were to use the funds allocated for the management of communications and marketing activities for corrupt purposes to obtain illicit benefits for the Company from public counterparties.

With reference to the activities envisaged above, the specific principles of conduct are indicated below.

To those who, by reason of their role or function or specific mandate, are involved in the aforementioned activities,**it is mandatory** Of:

- ensure compliance with company and group rules governing the processes listed above;

- ensure that company procedures include specific limitations relating to the characteristics of the hospitality, the duration of the events, the program and the contents;
- verify that the sponsorship of an event falls within the scope of a *budget* approved in accordance with company procedures;
- ensure that all events are approved according to the current delegation scheme;
- in the case of events organised by the Company with the support of third parties (agencies, organisers, etc.), ensure that the selection of the same always takes place in compliance with the provisions set out in the section "*Management of purchases of goods and services (including consultancy)*" of this chapter;
- ensure that gifts are of reasonable value, tied to a predefined commercial purpose and purchased and provided in compliance with company procedures;
- ensure the existence of a catalogue of goods/services that can be given away free of charge, with an indication of the cost of each item;
- validate any freebies not included in the catalogue;
- ensure the transparency and traceability of the approval and distribution process for free gifts;
- ensure the complete and correct archiving and recording, including through dedicated registers, of the freebies provided, indicating, among other things, the characteristics of the individual gadgets and the relevant recipients;
- ensure that donations and acts of generosity are approved by persons with appropriate powers;
- to foresee one screening of the hypothetical beneficiary of the donation, for the purposes of verifying the specific characteristics and integrity of the same;
- ensure the transparency and traceability of donations and charitable acts made;
- ensure that the documentation certifying the contribution disbursed is fully archived by the functions involved;
- ensure that relationships with counterparties are formalized through appropriate contractual instruments;
- to foresee a report periodical to be sent to the Supervisory Body regarding gifts, events, sponsorships and loans.

In the context of the aforementioned behaviour it **is forbidden** Of:

- distribute freebies and gifts outside of what is provided for by company practice: the permitted freebies are always characterised by their small value or because they are aimed at promoting charitable or cultural initiatives or the brand *image of* the Company. Gifts offered—except those of modest value—must be adequately documented to allow for verification by the Supervisory Board. In particular, any gift to Italian or foreign public officials or their family members that could influence their independence of judgment or induce them to secure any advantage for the company is prohibited;

- make charitable donations and sponsorships without prior authorization or outside of what is established by company practice; such contributions must be used exclusively to promote charitable or cultural initiatives or the brand *image of* the Group;
- promise or grant benefits to public/private entities, or to other subjects indicated by them, in order to ensure undue advantages for the Company;
- promise or provide benefits to Italian or foreign public officials, including sponsorships, for purposes other than institutional and service-related ones;
- offer or promise to Public Officials or their family members, directly or indirectly, any form of gift or free service that may appear to be connected to the business relationship with the Company, or aimed at influencing their independence of judgment, or inducing them to secure any advantage for the Company
- promise or grant contributions to persons whose names are included in the Lists available at the Bank of Italy, or to persons controlled by the latter, when such control relationship is known.

2.2 Sensitive Processes in the context of cybercrime and unlawful data processing and copyright infringement offences

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in Articles 24-*until* and 25-novies of Legislative Decree 231/01 are the following:

- Information Security Management; (Annex 3, Sheet 07)
- Management of internal and external communications (investors, advertising, etc.). (Annex 3, Sheet 09)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are listed in Appendix C to this Model. Appendix C also indicates the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory to** ensure that the aforementioned processes are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;

- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in Articles 24-*until* and 25-*novies* of Legislative Decree 231/2001 referred to above.

***

The main examples of crimes relating to the following activity are listed below:

- *Cybersecurity Management.*

The management of IT security could present risk profiles in relation to the configuration of computer crimes in the event that, for example, a senior executive or subordinate of the Company uses the IT tools made available by the Company to commit one of the crimes referred to in Article 24.*until* of Legislative Decree 231/2001.

The management of IT security could present risk profiles in relation to the configuration of crimes relating to copyright infringement in the event that, for example, a senior or subordinate individual of the Company, in order to obtain economic savings, installs software without having acquired the relevant licenses.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned process it **is mandatory** Of:

- ensure compliance with both local and Group IT operating procedures, which are an integral part of the corporate organizational model;
- for operations relating to access management,*accounting and* profiles, provide that:
  - formally define authentication requirements for systems for accessing data and for assigning remote access to them by third parties such as consultants and suppliers;
  - the identification codes (*user-id*) for access to applications and the network are individual and unique;
  - the assignment of the*Super User- ID*(SOUTH);
  - the correct use of the*Super User-ID;*
  - correct password management should be defined by guidelines, communicated to all users for the selection and use of passwords;
  - adequately inform users of IT systems of the importance of keeping their access codes confidential and not disclosing them to third parties; • the criteria and methods for creating passwords for accessing the network, applications, company information assets and critical or sensitive systems are defined (e.g. minimum password length, complexity rules, expiration);
  - access by users, in any manner, to data, systems and the network are subject to periodic checks;
  - applications track data changes made by users;
  - the criteria and methods for assigning, modifying and deleting user profiles are defined;

- administrator profiles are managed exclusively by individuals with specific powers;
- an authorization matrix is prepared – applications/profiles/applicant – aligned with the existing organizational roles;
- periodic checks of user profiles are carried out to verify that they are consistent with the assigned responsibilities;
- periodic checks are carried out to verify the actual use of the*account* and, in the event of user inactivity, proceed with the cancellation of the account;

- for operations concerning the management of telecommunication networks, provide that:
  - responsibilities for network management are defined;
  - security controls are implemented to ensure the confidentiality of data within the network and in transit on public networks;
  - network segregation and network traffic monitoring mechanisms are adopted;
  - mechanisms are implemented for tracking security events on networks (e.g. anomalous accesses in terms of frequency, modality, temporality);
  - the implementation and maintenance of telematic networks should be regulated by defining responsibilities and operating methods, and by periodically checking the functioning of the networks and any anomalies found;
  - periodic checks are carried out on the company's IT network, in order to identify anomalous behaviour such as, for example,*download* Of *files large-scale*, i.e. exceptional activities of servers outside of social operating hours;
  - the criteria and methods for backup activities are defined, which include, for each telecommunications network, the frequency of the activity, the methods, the number of copies, and the data retention period;
  - a plan should be defined*business continuity*and one of *disaster recovery* periodically updated and tested;
- for operations relating to systems management hardware, which also includes the management of the backup *and* the continuity of information systems and processes deemed critical, provide that:
  - the criteria and methods for managing the systems are defined*hardware*which provide for the compilation and maintenance of an updated inventory of the *hardware in* use at the Company and which regulate the responsibilities and operating methods in the event of implementation and/or maintenance of hardware;
  - the criteria and methods for the activities of backup *which* provide, for each application hardware, the frequency of the activity, the methods, the number of copies and the data retention period;
- for operations relating to systems management software, which also includes the management of the backup *and* the continuity of information systems and processes deemed critical, provide that:

- the criteria and methods for managing the systems are defined *software* which include the compilation and maintenance of an updated inventory of the software in use at the company, the use of *software* formally authorised and certified and carrying out periodic checks on the installed software and on the mass storage devices of the systems in use in order to check the presence of *software* prohibited and/or potentially harmful;
- the criteria and methods for the *change management* (intended as updating or implementing new technological systems/services);
- users of IT systems should be informed that the *software* assigned to them is protected by copyright laws and as such its duplication, distribution, sale or possession for commercial/entrepreneurial purposes is prohibited;
- to ban the *download* from unauthorized sources of *software* covered by *copyright*;
- the installation and use of is prohibited *software* not approved by the Company and not related to the professional activity carried out by the recipients or users;
- the installation and use of the following on the Company's IT systems is prohibited: *software* (c.d. "*P2P*", Of *files sharing* o in *istant messaging*) unauthorized through which it is possible to exchange with other subjects within the Internet any type of information *files* (such as videos, documents, songs, viruses, etc.) without any possibility of control by the Company;

- for operations concerning the management of physical access to the sites where the IT infrastructures are located, provide that:
  - the security measures adopted, the surveillance methods and their frequency, the responsibility, the process of reporting violations/break-ins of technical rooms or security measures, the countermeasures to be activated;
  - physical credentials for accessing the sites where the information systems and IT infrastructures are located are defined, such as, for example, access codes, *token authenticator*, pin, *badge*, biometric values and their traceability;
- for operations involving the management of digital signature devices, ensure that criteria and methods are defined for the generation, distribution, and revocation of the devices themselves, as well as controls to protect the devices from possible modifications or unauthorized use;
- in the event that IT security management is carried out - in whole or in part - with the support of third parties, ensure that the selection of the same always takes place in compliance with the provisions set out in the section *"Purchases of goods and services (including consultancy)"* of this Model and that they are subject to periodic monitoring by the ICT Function.

In the context of the aforementioned behaviour it **is forbidden** Of:
- use IT resources (e.g. *personal computer* fixed or portable) and network assigned by the Company for personal purposes or for purposes other than work;
- alter electronic documents, public or private, for evidentiary purposes;

- accessing, without authorization, a computer or telematic system or remaining there against the express or implied will of anyone who has the right to exclude him (the prohibition includes both access to internal information systems and access to the information systems of competing entities, public or private, for the purpose of obtaining information on commercial or industrial developments);
- procuring, reproducing, disseminating, communicating, or making known to third parties codes, passwords, or other means suitable for accessing another's computer or telematic system protected by security measures, or providing indications or instructions suitable for allowing a third party to access another's computer system protected by security measures;
- procure, produce, reproduce, import, disseminate, communicate, deliver or, in any case, make available to others computer equipment, devices or programs for the purpose of unlawfully damaging a computer or telematic system, the information, data or programs contained therein or pertaining to it, or of encouraging the total or partial interruption or alteration of its functioning (the prohibition includes the transmission of viruses with the purpose of damaging the information systems of competing entities);
- intercept, prevent or unlawfully interrupt computer or telematic communications;
- destroy, deteriorate, delete, alter or suppress information, data and computer programs (the prohibition includes unauthorized intrusion into the information system of a competitor company, with the aim of altering the latter's information and data);
- destroy, deteriorate, cancel, alter or suppress information, data and computer programs used by the State or another public body or pertinent to them or in any case of public utility;
- destroy, damage, render totally or partially unusable other people's computer or telematic systems or seriously hinder their functioning;
- destroy, damage, render, in whole or in part, unusable public utility computer or telematic systems or seriously hinder their functioning;
- install software/additional programs to those existing and/or authorized or without the appropriate licenses;
- damage or compromise in any way information, data and computer programs and/or entire computer or telematic systems of third parties, especially if they concern information and data used by the State or the Public Administration or computer or telematic systems of public utility;
- to duplicate illegally *software or* proprietary digital databases, using them on the Company's IT systems in violation of the relevant usage licenses.

The Company, in addition to preparing and communicating the procedures relating to the various IT activities, makes available in the *intranet company* regulations on the policies for the use and security of information systems which form an integral part of this Model.

***

The main examples of crimes relating to the following activity are listed below:

- *Management of internal and external communications (investors, advertising, etc.).*

The management of internal and external communications, and marketing activities in particular, could present risks related to copyright infringement if, for example, a senior executive or subordinate of the Company were to improperly use, for advertising purposes, intellectual property owned by others.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activity it **is mandatory** Of:

- ensure compliance with internal, EU and international regulations for the protection of intellectual property;
- use copyrighted works on the basis of agreements formalized in writing with the legitimate owner for their exploitation and in any case within the limits of said agreements;
- diligently handle the administrative obligations related to the use of works protected by copyright.

In the context of the aforementioned behaviors it is**prohibited** Of:

- disseminate and/or transmit, through websites, third-party works protected by copyright in the absence of agreements with the relevant owners, or in violation of the terms and conditions set forth in such agreements.

2.3 Sensitive Processes in the context of the crimes of receiving stolen goods, money laundering and use of money, goods or utilities of illicit origin, as well as self-laundering, organised crime crimes and crimes with the aim of terrorism or subversion of the democratic order

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in Articles 24-*to have* and 25-quarter and 25-octies of Legislative Decree 231/01 are the following:

- Customer Relationship Management; (Annex 3, Sheet 14)
- Management of purchases of goods and services (including consultancy); (Annex 3, Sheet 19)
- Management of gifts, donations, events, and sponsorships; (Annex 3, Sheet 16)
- Cash Flow Management; (Annex 3, Sheet 15)
- Relationship Management intercompany;(Annex 3, Sheet 01)
- Personnel Management and Reward System; (Annex 3, Sheet 11)
- Management of activities/remarketing; (Annex 3, Sheet 06)
- Selection and management of partner commercial; (Annex 3, Sheet 02)
- Accounting management, budget preparation, and tax management; (Annex 3, Sheet 08)

- Management of shareholders' meetings, capital transactions, and other non-routine transactions. (Annex 3, Sheet 17)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are listed in Appendix C to this Model. Appendix C also indicates the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph "General control environment", at the beginning of this section,**it is mandatory to** ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden** to carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in Articles 24-*to have* and 25-*quarter* and 25-*octies* of Legislative Decree 231/2001 referred to above.

***

The main examples of crimes relating to the following activities are listed below:

- *Customer relationship management;*
- *Management of remarketing activities.*

Customer relationship management could pose risks related to the commission of money laundering crimes if a senior or subordinate individual assists a customer in reintroducing money or other assets of illicit origin into the legal system.

Customer relationship management could present risks related to the commission of money laundering crimes if a senior or subordinate bank official fails to comply with anti-money laundering obligations, in order to avoid detecting deficiencies and/or irregularities in the information declared by a customer and/or in the documentation provided by the customer (for example, incomplete documents or documents containing false information, etc.). This omission could allow the establishment of an economic/financial relationship with individuals who use money of illicit origin in economic or financial activities or with individuals linked to terrorist organizations.

The management of customer relationships could present risks related to terrorist crimes in the event that, for example, a senior executive or subordinate of the Company were to provide financing to terrorist organizations or individuals connected to them.

The management of customer relationships could present risks related to organized crime if, for example, a senior executive or subordinate of the Company were to provide financing to individuals connected to criminal organizations.

Management of the activities of*remarketing*It could present risk profiles in relation to the crime of self-laundering in the event that, for example, a senior or subordinate individual, having committed or participated in committing the crime of bid-rigging in a tender procedure, uses, replaces, or transfers the proceeds deriving from the commission of this crime into economic, financial, entrepreneurial, or speculative activities, in such a way as to concretely hinder the identification of their criminal origin.

Management of the activities of *remarketing* It could present risk profiles in relation to the commission of money laundering crimes in the event that a senior or subordinate member of the bank fails to comply with anti-money laundering obligations, in order to avoid detecting deficiencies and/or irregularities in the information declared by a customer and/or in the documentation provided by the latter (for example, incomplete documents or documents containing false information, etc.), allowing, as a result of this omission, the establishment of an economic/financial relationship with individuals who use money of illicit origin in economic or financial activities or with individuals linked to terrorist organizations.

Management of the activities of*remarketing*It could present risk profiles in relation to organized crime if the Company were to enter into fictitious contracts or contracts with inconsistent values with individuals close to criminal organizations, in order to obtain economic and/or tax benefits.

Management of the activities of *remarketing* could present risk profiles in relation to crimes with terrorist purposes in the event that, for example, a senior or subordinate individual of the Company were to supply terrorist organizations or individuals connected to them with products that could also be used in terrorist activities.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activities, in addition to what is provided for in the
"Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority" of this Model,**it is mandatory** Of:

- ensure compliance with the policy and Group procedures on anti-money laundering;
- ensure the segregation of tasks between the different subjects involved in the process;
- identify and understand the customers and the individuals on whose behalf the customers operate (so-called beneficial owners);
- identify the beneficial owner(s) of the legal entity customer in accordance with the procedures established by the relevant legislation;
- ensure that customer due diligence is carried out on its counterparties and assign a consistent money laundering and terrorist financing risk profile;

- acquire and retain a copy of an original, non-expired identity document of the person undergoing due diligence;
- acquire information regarding the nature and purpose of the relationship or transaction;
- verify, if the client is a legal entity, the existence of the signatory's powers of representation by comparing them with a reliable and independent source (e.g. Cerved);
- proceed to verify the documentation, data or information obtained;
- verify the accuracy and completeness of the personal data and information relating to the economic activity carried out;
- verify the consistency between the person(s) included in the financing request as beneficial owner(s) and what appears in the *tool* computer scientists;
- verify the consistency between the requested financing and the client's economic and financial profile;
- check for any qualifications of a potential customer's Politically Exposed Person (PEP);
- obtain the client's declaration of qualification as a Politically Exposed Person;
- ensure that funding to individuals included in the Politically Exposed Persons lists is granted only after having carried out enhanced due diligence and only with prior authorization from the Director General or his delegate;
- check whether the name of the potential or existing customer is present within the*Black List*;
- ensure the use of IT control applications suitable for preventing operations in relation to countries or entities subject to financial and commercial restrictions (so-called "international sanctions");
- report any movements deemed anomalous to the relevant body, in order to proceed with the appropriate investigations and/or reports;
- evaluate the implementation of a Suspicious Transaction Report (SOS) after having ascertained the *status of* Potential Customer Terrorist;
- proceed with forwarding an SOS if it is not possible to comply with customer due diligence obligations;
- observe company procedures governing controls aimed at evaluating anomalous transactions and reporting suspicious transactions;
- ensure that no financing has been granted to entities for which the status of Terrorist;
- update existing customer information;
- constantly assess the risks of money laundering or terrorist financing according to the methods and timescales established by the assigned risk profile;
- prepare a specific one*report* external reserved for the Supervisory Authorities as well as reporting internal;

- ensure that all documentation relating to customer identification activities as well as periodic checks carried out on customer positions is adequately archived by the relevant bodies;
- ensure that any changes to the customer profile as well as the decision whether or not to forward a suspicious transaction report are adequately motivated and supported by appropriate documentation;
- ensure ongoing training for employees and collaborators on anti-money laundering and countering the financing of terrorism;
- in the event that the Company uses the support of third parties (consultants, lawyers, etc.) to fulfill its anti-money laundering obligations, ensure that their selection always takes place in compliance with the provisions set out in the section "*Management of purchases of goods and services (including consultancy)*".

In the context of the aforementioned behaviour it **is forbidden** Of:

- establish ongoing relationships, maintain existing ones and carry out transactions when it is not possible to comply with customer due diligence obligations;
- grant financing to individuals who have been identified as terrorists;
- carry out transactions for which there is a suspected risk of money laundering or terrorist financing;
- replace or transfer money, goods or other benefits deriving from illicit activities, or carry out other operations in relation to them, in such a way as to hinder the identification of their origin
- provide customers belonging to or in any case close to organised crime with financial resources, services or economic resources that could facilitate illegal activity;
- receive or conceal money derived from any crime and carry out activities that facilitate its acquisition, receipt or concealment.

***

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Management of purchases of goods and services (including consultancy);*
- *Selection and management of commercial partners;*
- *Personnel management and reward system;*
- *Financial flow management;*
- *Management of gifts, donations, events and sponsorships;*
- *Management of intercompany relationships.*

The management of purchases of goods and services (including consultancy) could present risks related to the crime of receiving stolen goods if the Company, in order to obtain an undue advantage, were to purchase goods of illicit origin.

The management of purchases of goods and services (including consultancy) could present risks related to the crime of self-laundering if, for example, invoices or other documents are recorded for non-existent transactions for the purpose of evading income or value added taxes, thus allowing the Company to build up funds of illicit origin to be used, replaced, or transferred to economic, financial, entrepreneurial, or speculative activities, thus effectively hindering the identification of the criminal origin.

The management of purchases of goods and services (including consultancy) could present risks related to the configuration of organized crime crimes if the Company were to enter into fictitious contracts or contracts with suppliers with intentionally inconsistent values associated with criminal organizations, in order to obtain economic and/or tax benefits.

A lack of transparency in the procurement process for goods and services could pose risks related to terrorist crimes, for example, if the Company, by transferring sums of money, provided financial support to organizations involved in terrorist or subversive activities.

The selection and management of *partner* commercial activities could present risk profiles in relation to the crime of organised crime in the event that the Company selects third parties affiliated with or close to a mafia-style criminal organisation.

The selection and management of partner/commercial activities could present risk profiles in relation to the crime of organised crime in the event that, for example, a senior or subordinate individual of the Company:

- entered into fictitious or deliberately inconsistent contracts with criminal organizations, in order to obtain economic and/or tax benefits;

- selected counterparts "close" to criminal organizations in order to obtain economic benefits;

- selected and hired personnel “close” to criminal organizations in order to obtain economic benefits.

A lack of transparency in the selection and management process*partner*commercial activities could present risk profiles relating to crimes with terrorist purposes in the event that, for example, the Company, by transferring sums of money, provided financial support to organizations involved in terrorist or subversive activities.

Personnel management could present risks related to organized crime if the Company, in order to receive an undue advantage, were to select an individual who has been reported to or is close to a criminal organization.

The management of financial resources, and specifically the receipt of payments, could present risks related to the crimes of receiving stolen goods, money laundering, and use of money if, for example, the Company accepts money from illicit activities.

A lack of transparency in the management of financial resources could pose a risk of committing the crime of self-laundering if, for example, it is possible to set aside financial

resources of illicit origin to be used, replaced, or transferred to economic, financial, entrepreneurial, or speculative activities, thereby effectively hindering the identification of their criminal origin.

The Financial flow management could present risks in relation to organized crime and terrorist offenses if, for example, the Company makes undue payments for services that are wholly or partially non-existent to third parties linked to criminal, mafia, or terrorist organizations in order to facilitate their illegal activities.

The management of gifts, donations, events, and sponsorships could pose risks related to organized crime if a subordinate or senior member of the Company relies on agencies/third parties connected to criminal organizations.

The management of gifts, donations, events, and sponsorships could pose risks related to terrorist crimes if a senior executive or subordinate of the Company sponsored and promoted charitable activities for individuals linked to terrorist organizations.

The relationship management*intercompany*It could present risk profiles in relation to the crimes of receiving stolen goods or money laundering in the event that the Company's attorneys, or other persons appointed by them, were to use financial resources in transactions with Group companies, in order to facilitate the introduction of money of illicit origin into the legal circuit.

For specific principles of conduct in relation to:

- *Management of purchases of goods and services (including consultancy);*
- *Selection and management of commercial partners;*
- *Personnel management and reward system;*
- *Financial flow management;*
- *Management of intercompany relationships;*
- *Management of gifts, donations, events and sponsorships.*

please refer to what is provided in the*"Sensitive Proceedings in Crimes against Public Administration and Crimes of Inducement to Withhold Statements or to Make False Statements to Judicial Authorities"*of this Model.

***

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Accounting management, budget preparation and tax management;*
- *Management of assembly activities, capital transactions and other non-routine operations.*

Tax management could present risks related to the crime of self-laundering if, for example, a senior or subordinate individual of the Company, using invoices or other documents for non-existent transactions to evade income or value added taxes, were to indicate fictitious liabilities in one of the annual tax returns relating to those taxes, thus constituting funds of illicit origin used, replaced, or transferred by the same individual in economic, financial, or entrepreneurial activities in such a way as to effectively hinder the identification of the criminal origin.

The management of capital transactions and other non-routine operations could present risks related to money laundering or self-laundering crimes if members of the Board of Directors, Auditors, or Shareholders were to carry out transactions using funds derived from illicit activities.

For specific principles of conduct in relation to:

- *Accounting management, budget preparation and tax management;*
- *Management of assembly activities, capital transactions and other non-routine operations*

please refer to what is provided in the*"Sensitive Proceedings in the Area of Corporate Crimes (including Private Bribery Crimes)".*

Furthermore, the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activities, are required to verify, before carrying out the transaction, that the counterparty is not present in the "*Black List*" or in the lists relating to financial and trade restrictions (so-called "international sanctions").

2.4 Sensitive Processes in the context of crimes involving non-cash payment instruments and fraudulent transfer of assets.

The Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in art. 25-*octies*.1 of Legislative Decree 231/01 are the following:

- Management of non-cash payment instruments (Annex C, Sheet 20);

Information security management. (Annex 3, Sheet 07);

- Customer Relationship Management; (Annex C, sheet 14);
- Management of activities/remarketing; (Annex C, sheet 06);
- Management of financial flows (Annex 3, Sheet 15);
- Management and assessment of customer credit.

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are listed in Appendix C to this Model. Appendix C also indicates the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph "General control environment", at the beginning of this section,**it is mandatory to** ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in art. 25-*octies*.1 of Legislative Decree 231/2001 referred to above.

***

The main examples of crimes relating to the following activity are listed below:

- *Management of non-cash payment instruments.*

The management of non-cash payment instruments could present risks in relation to the crime of improper use and counterfeiting of non-cash payment instruments where, for example, a Company representative improperly uses third-party credit cards or other non-cash payment instruments, without being the owner, in the interest of the Company.

Furthermore, the management of non-cash payment instruments could present risks related to the crime of computer fraud where, for example, a company representative alters the functioning of an IT system, resulting in a transfer of funds to the detriment of third parties and to the benefit of the Company.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activities,**it is mandatory** Of:

- ensure that the management process of non-cash payment instruments – including company credit cards (and other limited-use cards) – is carried out in compliance with the principle of segregation of roles and that specific controls are foreseen – in relation to the aforementioned instruments – regarding the issuance, delivery, replacement, renewal, activation, revocation, waiver or withdrawal activities of the Customer or Employee;
- ensure that the holders of the payment instruments and the payment authorization methods are clearly identified;
- ensure that, in the event that non-owners use non-cash business payment instruments, a delegation is granted with clear instructions and a precise scope of operations for the users;
- ensure constant monitoring and traceability of non-cash payment instruments issued by the Company to Customers or Employees;

- if they are in charge*outsource*or third parties in the management of payment instruments other than cash, contracts with such parties must contain a specific provision of knowledge of the legislation referred to in Legislative Decree 231/01 and a commitment to comply with it;
- Report to your manager any attempted counterfeiting or improper use of non-cash payment instruments by Employees, Customers, or third parties of which the Recipients become aware.

Furthermore, the Company ensures that training activities are carried out for Employees on the risks associated with the use of payment instruments other than cash and on the control procedures adopted.

In the context of the aforementioned behaviors it is prohibited Of:

- counterfeit, alter, or improperly use – without being the owner and for the purpose of making a profit for oneself or others (in particular, for the Company) – credit or payment cards, any document that enables the withdrawal of cash or the purchase of goods or services, and any other payment instrument other than cash;
- alter in any way the functioning of computer or telematic systems or intervene on the contents of said systems in order to carry out a transfer of money, monetary value or virtual currency.

***

The main examples of crimes relating to the following activity are listed below:

- *Cybersecurity Management.*

Cybersecurity management could present risks related to the crime of computer fraud where, for example, a company representative alters the functioning of an IT system, resulting in the transfer of funds to the detriment of third parties and to the benefit of the Company.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activity, in addition to what is provided for in the*"Sensitive Processes in the context of cybercrime and unlawful data processing and copyright infringement offences*" of this Model,**it is mandatory** Of:

- ensure the monitoring and traceability of physical equipment hardware in use at the Company;
- provide locking systems in relation to the installation and use of*hardware*and*software*not approved and not related to the professional activity carried out by individual employees;
- carry out periodic checks to identify any installations of unauthorized programs, including the forced removal of any unauthorized content.

In the context of the aforementioned behaviors it is prohibited Of:

- alter in any way the functioning of computer or telematic systems or intervene on the contents of said systems in order to carry out a transfer of money, monetary value or virtual currency;

- unlawfully entering, directly or through a third party, a computer or telematic system protected by security measures against the will of the holder of the right of access, including for the purpose of improperly using, falsifying or altering payment instruments other than cash.

- *Customer Relationship Management; (Annex C, sheet 14)*
- *Management of remarketing activities; (Annex C, sheet 06)*

Customer relationship management and management of business activities*remarketing*could present risk profiles in relation to the crime of fraudulent transfer of assets in the event that a subordinate or senior member of the Company contributes, through financial and currency movements, to the transfer of ownership of money or other assets in order to evade legal provisions regarding asset prevention measures, smuggling, or to facilitate the substitution of the transfer of capital of illicit origin.

The Recipients as defined above who, by reason of their role or function, are involved in the management of the aforementioned activities it **is mandatory** Of:

- ensure, where necessary, that customer relationships are managed exclusively by persons with appropriate powers;
- ensure compliance with all provisions of the *policy and* Group procedures, particularly those relating to anti-money laundering, antitrust and conflict of interest;
- ensure the traceability of all phases of the commercial process, including the definition of financial conditions, any discounts applied, and the duration of agreements, through the use of the required information systems;
- provide for adequate segregation of tasks and responsibilities in customer management, with particular reference to the definition of financial conditions and payment methods and times;
- ensure that commercial offers/proposals are defined on the basis of company procedures;
- ensure that relationships with customers are formalized in specific written agreements (e.g. commercial offers/proposals), approved by persons with specific powers;
- ensure that preliminary screening is carried out on the new client, both in terms of compliance, including anti-money laundering and creditworthiness;
- ensure the segregation of functions in all phases relating to the management of customer relations and the management of sales activities *remarketing*, including the creation of customer records; ensuring that any exceptions to the financial conditions, determined automatically through the use of a specific system, are authorized in compliance with the provisions of the system of delegations and powers of attorney;
- ensure the traceability of all phases of the sales entity agreement process;
- carry out specific verification activities related to credit management;
- ensure the traceability of all documentation sent to customers;
- verify the regularity of invoicing towards customers;

- carry out a specific analysis of complaints received from customers;
- forward the financing application to the competent signature level for the approval;
- in the event that the services provided to customers are carried out - in whole or in part - with the support of third parties, ensure that their selection always takes place in compliance with the provisions set out in the "Selection and Management of Commercial Partners" section of this chapter;
- promptly communicate to their immediate superior or to the Company's management and, at the same time, to the Supervisory Body any conduct carried out by those working for the counterparty, aimed at obtaining financial or currency transfers which, given the manner in which they are intended to be carried out, appear to be such as to obtain transfers of values in violation of the current regulations for the prevention and fight against money laundering or terrorist financing.

In the context of the aforementioned behaviour it **is forbidden** Of:

- make services or payments to third parties that are not adequately justified in the context of the contractual relationship established with them;
- submit offers that have not been subjected to the approval process required by company procedures;
- enter into contracts with conditions established according to non-objective parameters and/or in violation of the provisions of company procedures and relevant legislation;
- submitting untrue statements by presenting documents that do not correspond in whole or in part to reality or by omitting to present real documents;
- grant credit outside the circumstances contemplated by company credit policies.

- *Cash Flow Management (Annex 3, Sheet 15)*
- *Management and evaluation of customer credit*

The management of financial flows and the management and assessment of customer credit may present risks related to the crime of fraudulent transfer of assets if a subordinate or senior executive of the Company contributes, through financial and currency transactions, to the transfer of ownership of money or other assets in order to evade legal provisions regarding asset prevention measures, smuggling, or to facilitate the substitution of the transfer of capital of illicit origin.

With reference to the activities envisaged above, the specific principles of conduct are indicated below.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of financial flows and in the management and evaluation of credit towards customers it **is mandatory** Of:

- ensure that the management of financial resources is carried out in accordance with the rules defined by the Company;

- authorize only previously identified individuals with specific power of attorney to manage and move financial flows;
- ensure a payment approval process, in accordance with the Bank's system of delegations and powers of attorney;
- carry out procedural controls with reference to financial management, with particular attention to flows that do not fall within the company's typical processes and which are therefore managed in an extemporaneous and discretionary manner, in order to prevent the formation of hidden reserves;
- ensure the evaluation and monitoring of investments made;
- ensure that all provisions relating to bank accounts held in the Company's name, as well as payments made using other methods (e.g., company credit cards), are adequately documented and authorised in accordance with the current delegation system;
- monitor bank reconciliations on a monthly basis;
- when using the funds in the petty cash box, comply with internal company rules as well as the limits on the use of cash set out in current legislation;
- establish limits on the autonomous use of financial resources by defining quantitative thresholds consistent with the organizational roles and responsibilities assigned to individuals;
- carry out all financial flow movements with tools that guarantee their traceability;
- ensure that, for the management of incoming and outgoing flows, only the channels of banks and other accredited financial intermediaries subject to European Union regulations or credit/financial institutions located in a non-EU country are used, which impose obligations equivalent to those required by anti-money laundering laws and provide for the monitoring of compliance with such obligations;
- ensure adequate segregation between those who can upload payment slips, the approvers, and those who manage sensitive data within supplier databases;
- ensure that banking operations, such as opening and closing the Company's bank accounts and other dispositive operations, are authorised only by persons with adequate powers;
- ensure that the documentation is signed by persons with appropriate powers; evaluate credit towards customers through the use of credit management systems *rating;*
- ensure that credits are written off only on the basis of internal policies and procedures, reliable documentation certifying the actual irrecoverability of the credit, and in accordance with accounting principles and tax regulations;
- where third parties are used for credit management, ensure that relationships with the aforementioned parties are formalised through written contracts containing clauses specifying: that the third party declares that it respects the principles set out in Legislative Decree 231/2001, as well as adhering to the principles of the company's Code of Conduct;

- that the third party declares that it has implemented all necessary measures and precautions aimed at preventing the crimes indicated above, having equipped its corporate structure – where possible – with internal procedures and systems that are fully adequate for such prevention;
- that the untruthfulness of the aforementioned declarations could constitute grounds for termination of the contract pursuant to art. 1456 of the Italian Civil Code;

- ensure that the selection of any third parties takes place in compliance with the provisions set out in the section "*Management of purchases of goods and services (including consultancy)"*of this chapter;
- ensure that documentation is archived at the functions involved in the process;
- communicate, without delay, to *management companies* and, at the same time, the Supervisory Body, any critical issues that may arise within the scope of the activity in question.
- report to the Supervisory Body, on a six-monthly basis, the results of the checks carried out on incoming and outgoing financial flows, indicating any anomalies found (for example, lack of supporting documentation, flows relating to purposes not related to the company's activity, etc.).

In the context of the aforementioned behaviors **it is forbidden** Of:

- make cash payments for amounts exceeding regulatory limits or with untraceable payment methods;
- make payments to numbered current accounts or accounts not in the name of the supplier;
- make payments to current accounts other than those contractually provided for;
- making payments that are not properly documented;
- receive payments from parties who have no commercial/contractual relationship with the Company, except in specific cases governed by company procedures;
- create funds for unjustified payments (in whole or in part), including through relationships with companies belonging to the Group;
- create or allow the creation of illicit, hidden or otherwise incorrectly accounted funds, through any illicit, simulated, fictitious and/or incorrectly accounted financial operation or movement;
- make transfers of cash or bearer bank or postal deposit books or bearer securities in euros or foreign currency, when the value of the transaction, even if split, is overall equal to or greater than the limit established by the Anti-Money Laundering Regulations;
- make requests for the issuance and use of free-form bank and postal cheque forms, in place of those with a non-transferability clause;
- issue bank and postal checks that do not indicate the name or company name of the beneficiary and do not contain a non-transferability clause;

- open accounts or savings books anonymously or under fictitious names and use those opened in foreign countries;
- make bank transfers without indicating the counterparty;
- make money transfers for which there is no full correspondence between the recipients/payers and the counterparties actually involved in the transactions;
- make payments or recognize compensation in favor of third parties operating on behalf of the Company, which are not adequately justified in the context of the contractual relationship established with them;
- make payments to/from an account other than the one indicated in the account details or relating to credit institutions based in tax havens or which do not have physical establishments in any country;
- make payments to/from counterparties based in tax havens, countries at risk of terrorism, etc.;
- authorize the transfer to loss of credits without the requirements being met;
- enter into relationships with parties attributable to contracting authorities, or with third parties participating in public tenders called by the same contracting authorities, with the aim of unduly interfering in the definition of the tender notice or in the award procedures.

2.5 Sensitive processes in the context of crimes of counterfeiting of money, public credit cards, stamps and instruments or signs of recognition and in crimes against industry and commerce

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in Articles 25-*until* and 25-*until* I of Legislative Decree 231/01 are the following:

- Management of activities *remarketing*; (Annex C, Sheet 06)
- Management of development activities; (Annex C, Sheet 05)
- Management of internal and external communications (investors, advertising, etc.). (Annex C, Sheet 09)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are listed in Appendix C to this Model. Appendix C also indicates the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory** to ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden** to carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in Articles 25-*until* and 25-*until* I of Legislative Decree 231/2001 referred to above.

***

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Management of remarketing activities.*

Management of the activities of remarketing could present risk profiles in relation to the crime of fraud in the exercise of commerce in the event that, for example, a subordinate or senior member of the Company delivers to the customer a product of a different quality than that declared or agreed upon in the agreement.

For specific principles of conduct in relation to:

- *Management of remarketing activities.*

please refer to what is provided in the*"Sensitive Proceedings in Crimes against Public Administration and Crimes of Inducement to Withhold Statements or to Make False Statements to Judicial Authorities"*of this Model.

***

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Management of development activities;*
- *Management of internal and external communications (investors, advertising, etc.).*

The management of new service development activities could present risks related to the crime of forgery of identifying instruments or signs in the event that, for example, a senior executive or subordinate of the Company, being aware of the existence of an industrial property right, counterfeits or alters national or foreign trademarks or distinctive signs of industrial products, or, without being involved in the counterfeiting or alteration, uses such counterfeit or altered trademarks or signs.

The management of internal and external communications, particularly marketing activities, as well as the management of new service development activities, could pose risks related to crimes against industry and commerce if, for example, the Company were to use fraudulent

means, such as artifice, deception, and lies, to mislead a customer when promoting new products and services. These could also include the use of other people's registered trademarks, the dissemination of false and misleading information, and false advertising.

The management of internal and external communications, and marketing activities in particular, could present risks related to the crime of forgery of identifying instruments or signs, for example, if a senior executive or subordinate of the Company were to improperly use, for advertising purposes, a pre-existing trademark or distinctive sign owned by others.

With reference to the activities envisaged above, the specific principles of conduct are indicated below.

To the Recipients as defined above who, by reason of their role or function or mandate, are involved in the management of research and development activities it **is mandatory** Of:

- ensure compliance with internal, EU and international regulations protecting industrial property rights, patents, designs or models;
- ensure adequate segregation of duties regarding development activities;
- verify the absence of possible violations of third-party rights in the development of new services and in communication activities;
- ensure systematic monitoring of the legislation in force in this area.

In the context of the aforementioned behaviour it **is forbidden** Of:

- use or market products and services with third-party industrial property rights in the absence of agreements with the relevant owners, or in violation of the terms and conditions set forth in such agreements;
- realize any conduct aimed, in general, at the production and marketing of products protected by third-party industrial property rights.

2.6 Sensitive Processes in the context of corporate crimes (including corruption crimes between private individuals)

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in art. 25-*to have* of Legislative Decree 231/01 are the following:

- Management of administrative obligations, relations with Supervisory Authorities, and related inspection activities; (Annex C, Sheet 18)
- Accounting management, budget preparation, and tax management; (Annex C, Sheet 08)
- Management of assembly activities, capital transactions and other non-routine operations; (Annex C, Sheet 17)
- Management of relationships with corporate bodies; (Annex C, Sheet 13)
- Management of internal and external communications (investors, advertising, etc.). (Annex C, Sheet 09)

With specific reference to corruption crimes between private individuals, the Company has also identified the following Sensitive and Instrumental Processes:

Sensitive Processes

- Customer Relationship Management; (Annex C, sheet 14)
- Management of activities *remarketing*; (Annex C, sheet 06)
- Management of litigation and relations with the Judicial Authority and management of settlement agreements; (Annex C, sheet 12)

Instrumental Processes

- Management of purchases of goods and services (including consultancy); (Annex C, sheet 19)
- Selection and management of *partner* commercial. (Annex C, sheet 02)
- Personnel Management and Reward System; (Annex C, Sheet 11)
- Management of expense reports and entertainment expenses; (Annex C, sheet 04)
- Financial Flow Management; (Annex C, sheet 15)
- Management and assessment of customer credit; (Annex C, sheet 03)
- Relationship Management *intercompany*; (Annex C, sheet 01)
- Management of gifts, donations, events, and sponsorships; (Annex C, sheet 16)
- Management of internal and external communications (investors, advertising, etc.); (Annex C, sheet 09)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are listed in Appendix C to this Model. Appendix C also indicates the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory** to ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in art. 25-*to have* of Legislative Decree 231/2001 referred to above.

***

Specific principles of conduct relating to corporate crimes

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Accounting management, budget preparation and tax management;*
- *Management of internal and external communications (investors, advertising, etc.).*

Accounting management and financial statement preparation could present risks related to the crime of false corporate reporting, for example through the approval of untrue financial statements, also due to incorrect management, recording, aggregation, and evaluation of accounting data.

Accounting management could pose risks related to corporate crimes if the Company were to modify accounting data present in company systems in order to provide a false representation of the financial position, economic performance, and assets through the inclusion of non-existent balance sheet items or values that differ from the actual ones.

The management of internal and external communications (investors, advertising, etc.) could present risks related to the crime of false corporate communications if, for example, the Director or Manager responsible for preparing accounting documents knowingly discloses materially untrue facts or omits materially relevant facts, whose disclosure is required by law, regarding the economic, financial, or asset situation of the company or group, in a manner likely to mislead others.

To the Recipients as defined above who, by reason of their role or function or mandate, are involved in the management of accounting, in the preparation of the financial statements and related attachments, in the management of taxation or in internal and external communications **it is mandatory** Of:

- maintain correct, transparent, and collaborative behavior, in compliance with the law, applicable accounting principles, and internal rules, in all activities aimed at preparing the financial statements and other corporate communications, in order to provide truthful and accurate information on the Company's economic, financial, and fiscal situation;
- ensure the strictest accounting transparency at all times and under any circumstances;
- carry out all communications (addressed to customers, the market, and the press) in compliance with the principles of good faith, truthfulness, correctness, and transparency;
- clearly and completely identify the functions affected by the communications, as well as the data and information that they must provide;
- Provide the necessary training on the main legal and accounting concepts and issues related to financial statements for managers of the functions involved in preparing the financial statements and other related documents, particularly focusing on the training of new hires and the provision of periodic refresher courses;

- strictly observe all provisions established by law to protect the integrity and effectiveness of the share capital, in order not to undermine the guarantees of creditors and third parties in general;
- observe the rules of clear, correct and complete recording in the accounting activity of facts relating to the management of the Company;
- ensure the completeness and accuracy of accounting closings;
- ensure compliance with company rules relating to the preparation of statutory and consolidated financial statements;
- ensure compliance with the rules of segregation of duties between the person who carried out the operation, the person responsible for recording it in the accounts and the person carrying out the related control;
- ensure compliance with obligations (both in terms of tax returns and payments) and deadlines set by tax legislation;
- ensure that the draft budget is subject to verification by all company functions required by company procedures;
- to base relations with the Supervisory Authorities, including the tax authorities, on maximum transparency, collaboration, availability and in full compliance with the institutional role played by them and with the existing legal provisions on the matter, the general principles and rules of conduct referred to in the Code of Conduct as well as in this part of the Model;
- promptly implement the provisions of the same Authorities and the required formalities;
- ensure that the documentation to be sent to the Supervisory Authorities is produced by competent and previously identified persons;
- use accounting systems that guarantee the traceability of individual transactions and the identification of users who enter data into the system or modify its contents;
- ensure compliance with the requirements of the legislation on direct and indirect taxes; ensure that all relationships intercompany are formalized through specific contracts;
- ensure the proper functioning of the Company and its corporate bodies, guaranteeing and facilitating all forms of internal control over corporate management required by law, as well as the free and correct formation of the assembly's will;
- comply with the procedure that regulates the evaluation and selection phases of the auditing firm;
- assign consultancy tasks having as their object activities other than accounting auditing to the auditing firm or to the companies or professional entities belonging to the same *network of* the auditing firm, exclusively in compliance with current legislation;
- Where third parties (companies, consultants, professionals, etc.) are used to manage activities, ensure that relationships with them are formalized through written contracts containing clauses specifying:

- that the third party declares that it respects the principles set out in Legislative Decree 231/2001, as well as adhering to the principles of the company Code of Conduct;
- that the third party declares that it has implemented all necessary measures and precautions aimed at preventing the crimes indicated above, having equipped its corporate structure – where possible – with internal procedures and systems that are fully adequate for such prevention;
- that the untruthfulness of the aforementioned declarations could constitute grounds for termination of the contract pursuant to art. 1456 of the Italian Civil Code;

- refrain from spreading false information or carrying out fraudulent transactions that may or may not deceive the public regarding the Bank's true situation, thus impacting - to the benefit or interest of the institution - the trust that third parties have in its stability;
- ensure that the disclosure of external information occurs in compliance with company procedures.

In the context of the aforementioned behaviors it is **prohibited** Of:

- carry out actions aimed at providing misleading information with reference to the actual representation of the Company, failing to provide a correct representation of the economic, patrimonial, financial and tax situation of the Company;
- omit data and information required by law on the economic, patrimonial and financial situation of the Company;
- return contributions to members or release them from the obligation to make them, except in cases of legitimate reduction of the share capital;
- carry out reductions in share capital, mergers or demergers in violation of the provisions of law protecting creditors;
- proceed in any way to the fictitious formation or increase of the share capital;
- carry out transactions, including with Group companies, in order to evade tax regulations;
- alter or destroy financial and accounting documents and information available online through unauthorized access or other actions suitable for the purpose;
- submitting false statements to the Supervisory Authorities, exhibiting documents that do not correspond in whole or in part to reality;
- use Inside Information based on one's position within the Group or due to the fact of having a business relationship with the Group, to trade, directly or indirectly, financial instruments of a Group company, of client or competitor companies, or of other companies to gain a personal advantage, as well as to favor third parties or the company or other Group companies;
- disclose to third parties Inside Information relating to the Group, except in cases where such disclosure is required by law, other regulatory provisions or specific contractual agreements whereby the counterparties have undertaken in writing to use it exclusively for the purposes for which such information is transmitted and to maintain its confidentiality;

- participate in discussion groups or *chatrooms on* the Internet concerning financial instruments or issuers of financial instruments, whether listed or unlisted, and in which there is an exchange of information concerning the Group, its companies, competing companies or listed companies in general or financial instruments issued by such entities, unless these are institutional meetings for which a verification of legitimacy has already been carried out by the competent functions or there is no exchange of information whose non-privileged nature is evident;
- leave documents containing Inside Information in places where they could easily be read by people who are not authorized, under company procedures, to know such information.

***

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Management of assembly activities, capital transactions and other non-routine operations;*
- *Management of relationships with corporate bodies.*

The management of assembly activities could present risks related to the crime of illicit influence on the assembly, in the event that a majority in the assembly were to be achieved in any way through simulated or fraudulent actions, for example through the presentation of false or misleading documents or information.

The management of shareholders' meetings, capital transactions, and other non-routine operations could present risks related to the configuration of corporate crimes in the event that, for example, the Company's Directors or Auditors, through capital transactions or improper management of shareholders' meetings, were to take actions to the detriment of the Company's shareholders.

The management of shareholders' meetings, capital transactions, and other non-routine operations could also present risks related to the crime of obstructing the exercise of the functions of public supervisory authorities, for example, if directors disclose material facts that are not true in communications to the public supervisory authorities required by law, with the aim of obstructing their activity.

Capital transactions and other non-routine transactions could present risks related to the crimes of undue restitution of contributions, illegal distribution of profits or reserves, illicit transactions involving shares or company quotas, and fictitious formation of capital if members of the Board of Directors, Auditors, or Shareholders were to carry out illicit transactions that affect the Company's assets.

The management of relationships with corporate bodies could present risks related to the commission of the crime of obstruction of control in the event that, for example, a subordinate or senior member of the Company, by concealing documents or implementing other suitable artifices, prevented or otherwise hindered the performance of control activities legally attributed to shareholders or other corporate bodies.

All corporate formalities (calling meetings, maintaining company books, administrative procedures, etc.) are handled by the Corporate Affairs department, according to the procedures and timelines established by law. The Corporate Affairs department is responsible for drafting the minutes of meetings and maintaining company books.

All documentation must be archived by the functions involved in the process in accordance with company rules and applicable legislation.

Capital and/or non-routine transactions are resolved and approved by the Board of Directors and/or the Shareholders' Meeting.

With regard to the management of assembly activities, capital transactions, and other non-routine operations, the parties involved must ensure the proper functioning of the Company and its corporate bodies, guaranteeing and facilitating the free and correct expression of the assembly's will.

Recipients who, by reason of their role or function or mandate, are involved in the management of assembly activities, capital transactions and other non-routine transactions and in the management of relations with corporate bodies are required to **obligation** Of:

- ensure the proper functioning of the corporate bodies, guaranteeing and facilitating the free and correct formation of the assembly's will;
- ensure compliance with the rules of segregation of duties between the subjects involved in the management of the activities;
- adopt specific measures to ensure that the organization of the Assembly, the assembly proceedings, and post-assembly procedures are implemented in accordance with the provisions of current legislation regarding assembly procedures;
- prepare documents relating to assembly resolutions and the convening of corporate bodies in a clear and precise manner;
- ensure that administrative and accounting requirements relating to capital transactions and other non-routine transactions are managed with the utmost diligence and professionalism, avoiding conflicts of interest;
- comply with all provisions established by law to protect the integrity and effectiveness of the share capital, in order not to undermine the guarantees of creditors and third parties in general;
- ensure that the exclusive power to decide on the completion of transactions such as (for example): purchases, sales, mergers, investments, divestments or assumption of commitments in general by the Bank and its directly or indirectly controlled companies of strategic importance, is vested - within the limits set by the Articles of Association - in the Board of Directors;
- ensure the proper functioning of the corporate bodies by allowing for any internal controls;
- maintain the utmost diligence, professionalism, transparency, collaboration, and availability in managing relationships with the Board of Statutory Auditors and the Independent Auditors, and ensure full respect for their roles;

- make available data and documents requested by the supervisory bodies in a timely manner and in clear, objective and comprehensive language in order to provide accurate, complete, truthful and truthful information.

With reference to extraordinary financial transactions (typically referring to the issuance of bonds, the assumption of loans and financing, the subscription and increases in share capital, the granting of guarantees and sureties, the granting of financing and the subscription of bonds, the acquisition of business units or shareholdings, and other extraordinary transactions such as mergers, demergers, and contributions), the parties involved must ensure that: the competent body, be it the Board of Directors or another formally delegated person, has adequate information support to be able to make an informed decision.

For each extraordinary financial transaction to be approved, the delegated function is required to prepare documentation suitable for assessing its feasibility and strategic and economic suitability, including, where applicable:

- qualitative and quantitative description of the target (feasibility study, financial analysis, studies and statistics on the reference market, comparisons between different alternatives for carrying out the operation);
- characteristics and subjects involved in the operation, also through analysis of *compliance on* the same;
- technical structure, main guarantees and collateral agreements and financial coverage of the operation;
- methods for determining the economic conditions of the operation and indication of any external consultants/intermediaries/advisors involved;
- impact on the prospective economic, financial and equity situation;
- assessments regarding the appropriateness and compliance of the transaction to be approved with the Company's interests.

In the context of behaviors it is **prohibited to** carry out, during meetings, simulated or fraudulent acts aimed at altering the regular process of forming the assembly's will. Furthermore,**it is forbidden** Of:

- return contributions to members or release them from the obligation to make them except in cases of legitimate reduction of share capital;
- distribute profits or advances on profits not actually earned or legally allocated to reserves, or distribute reserves, even if not constituted with profits, which cannot by law be distributed;
- purchase or subscribe - outside the cases provided for by law - own shares, or shares of controlled companies, thereby damaging the integrity of the share capital or reserves that are not distributable by law;
- carry out reductions in share capital, mergers, and demergers with other companies, in violation of the provisions of the law protecting creditors, causing damage to the latter;

- proceed with the fictitious formation or increase of share capital by: (i) attribution of shares or quotas in an amount that is overall greater than the amount of the share capital, (ii) reciprocal subscription of shares or quotas, (iii) significant overvaluation of contributions of assets in kind or credits or of the Bank's assets in the event of transformation;
- divert company assets among the members during the liquidation of the Bank before paying the company's creditors or setting aside the sums necessary to satisfy them, causing damage to the aforementioned creditors;
- engage in misleading conduct that could lead the Board of Statutory Auditors or the Auditing Firm to make an error in the technical-economic evaluation of the documentation presented;
- present incomplete documents and false or altered data.

***

The main examples of crimes with reference to the following Sensitive Process are listed below:

- *Management of administrative obligations, relations with Supervisory Authorities, and related inspection activities.*

The management of administrative obligations, relationships with Supervisory Authorities, and related inspection activities could present risks related to the crime of obstructing the exercise of the functions of public supervisory authorities if, for example, the Company's directors disclosed material facts that were untrue in communications to the public supervisory authorities required by law, with the aim of obstructing their activity.

The management of relationships, communications, and the provision of documentation requested by the Supervisory Authorities (Bank of Italy, Consob), including following inspections, could present risks related to the commission of the crime of obstructing the exercise of the functions of public supervisory authorities if, for example, a senior person or subordinate of the Bank were to provide incorrect data or conceal information that should be reported to the Authority.

For specific principles of conduct in relation to the above-mentioned sensitive area, please refer to the provisions in*"Sensitive Proceedings in Crimes against Public Administration and Crimes of Inducement to Withhold Statements or to Make False Statements to Judicial Authorities"*of this Model.

***

<u>Specific principles of conduct relating to corruption crimes between private individuals</u>

The main examples of crimes with reference to the following Sensitive Processes are listed below:

- *Customer relationship management;*
- *Management of remarketing activities;*

Customer relationship management and management of business activities*remarketing*could present risk profiles in relation to the crime of corruption between private individuals in the event that a subordinate or senior member of the Company offers or promises money or other benefits to the head of the purchasing office of a client company in order to obtain the stipulation of a contract for the supply of a product or service at a price higher than the market price or under particularly unfavourable conditions compared to the *standard* normally in use.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes with reference to the following Sensitive Process are listed below:

- *Litigation management and relations with the Judicial Authorities and management of settlement agreements.*

The management of settlement agreements could present risks in relation to the crime of corruption between private individuals where a company representative (or even a consultant, such as a lawyer) bribes the legal representative or counsel of the opposing party (for example, a corporation) in order to obtain a resolution of the dispute in their favor (for example, through the opposing party's withdrawal from the litigation or by reaching a settlement agreement out of court on more advantageous terms).

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes with reference to the following Instrumental Process are listed below:

- *Management of purchases of goods and services (including consultancy).*

The management of purchases of goods and services (including consultancy) could present risks related to the crime of corruption between private individuals if, for example, a senior executive or subordinate of the Company provides money or other benefits (e.g., gifts, hiring, etc.) to the purchasing manager of a supplier company in order to obtain the supply of a good or service at a price below the market price or under particularly favorable conditions compared to the standards normally in use.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes with reference to the following Instrumental Process are listed below:

- *Selection and management of commercial partners.*

The selection and management of *partner* commercial activities could present risk profiles in relation to corruption crimes in the event that, for example, a subordinate or senior member of the Company stipulates fictitious contracts or contracts with values that are deliberately not in line with *partner in* order to create funds to be used for corrupt purposes.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes relating to the following activity are listed below:

- *Personnel management and reward system.*

Personnel management could present risks related to the crime of corruption between private individuals in the event that, for example, a senior executive or subordinate of the Company hires an employee from a competing company in exchange for information useful to the Company (industrial secrets, etc.).

The management of the reward system could present risks related to the crime of corruption, in the event that the Company provides a resource with cash bonuses/incentives that are intentionally disproportionate to their role/skills, in order to provide the employee with the funds to carry out corrupt acts.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes relating to the following activity are listed below:

- *Management of expense reports and entertainment expenses.*

The management of expense reports could present risks related to corruption crimes between private individuals, in the event that the Company, in order to provide employees with supplies to be used for corrupt purposes, reimbursed fictitious expenses or expenses not falling within the employee's normal business activities.

The management of entertainment expenses could present risks related to corruption crimes, for example, if a senior executive or subordinate of the Company were to use sums subsequently accounted for as entertainment expenses to bribe a private counterparty.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public*

*Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes with reference to the following Instrumental Processes are listed below:

- *Financial flow management;*
- *Management and evaluation of customer credit;*
- *Management of intercompany relationships.*

The lack of transparency in the management of financial resources could pose risks related to corruption crimes between private individuals, for example, if the Company were allowed to set aside funds for corruption purposes.

The management and assessment of customer credit could present risks related to the crime of corruption between private individuals if, for example, a subordinate or senior executive of the Company authorizes a write-off of credit, even without the requirements, in order to grant a benefit to the counterparty and create funds to be used for corruption purposes.

Relationship management*intercompany*It could present risk profiles in relation to the crime of corruption between private individuals in the event that the Company were to use financial resources in transactions with Group companies in order to create funds to be used for corrupt purposes.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

***

The main examples of crimes relating to the following activities are listed below:

- *Management of gifts, donations, events and sponsorships;*
- *Management of internal and external communications (investors, advertising, etc.).*

The management of gifts, donations, events, and sponsorships could pose risks related to the crime of corruption if a senior executive or subordinate of the Company grants gifts of significant value to private counterparties in order to commit corrupt acts and obtain illicit benefits.

The management of internal and external communications (investors, advertising, etc.) could present risk profiles in relation to corruption crimes in the event that a senior or subordinate individual of the Company were to use the funds allocated for the management of communication activities and *marketing for* corrupt purposes to obtain illicit benefits, in favor of the Company, from public or private counterparts.

Reference is made, where applicable, to the principles of conduct set out in the*"Sensitive/Instrumental Proceedings in the context of crimes against the Public*

*Administration and crimes of inducing individuals not to make statements or to make false statements to the Judicial Authority"*of this Model.

2.7 Sensitive Processes in the context of crimes of*Market Abuse*and administrative offenses

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in art. 25-sexies of Legislative Decree 231/01 and art. 187-*quinquies of* the T.U.F. are the following:

- *Management of internal and external communications (investors, advertising, etc.).*

The Corporate Functions/Departments involved in the Sensitive Process listed above and falling within the specific Crime Family are identified in Annex C to this Model. Annex C also contains the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory to** ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in art. 25-Sexies of Legislative Decree 231/2001 and art. 187-*quinquies*of the T.U.F. previously recalled.

***

The main examples of crimes with reference to the following Sensitive Process are listed below:

- *Management of internal and external communications (investors, advertising, etc.).*

The management of internal and external communications (investors, advertising, etc.) could present risks related to the crime of insider dealing and market manipulation in the event that, for example, a subordinate or senior member of the Company, possessing inside information as a result of their work, buys, sells, or carries out other transactions, directly or indirectly, on their own behalf or on behalf of third parties, in financial instruments using that information.

To the Recipients as defined above who, by reason of their role or function or mandate, are involved in the management of internal and external communications **it is mandatory** Of:

- ensure that the handling of Inside Information is carried out in compliance with the relevant internal procedures of the Company or Group;
- ensure compliance with the principle of segregation of roles in the management of Inside Information and the management of external communications, in line with the delegation system adopted by the Company;
- ensure the confidentiality of information through adequate confidentiality measures aimed at ensuring the organizational, physical and logical security of the information itself;
- ensure the completeness and exhaustiveness of the list of persons having access to Inside Information;
- transmit the list of persons having access to Inside Information to the competent Authorities upon their specific request.

In the context of the aforementioned behaviors it is prohibited Of:

- use Inside Information based on one's position within the Group or due to the fact of having a business relationship with the Group, to trade, directly or indirectly, financial instruments of a Group company, of client or competitor companies, or of other companies to gain a personal advantage, as well as to favor third parties or the company or other Group companies;
- disclose to third parties Inside Information relating to the Group, except in cases where such disclosure is required by law, other regulatory provisions or specific contractual agreements whereby the counterparties have undertaken in writing to use it exclusively for the purposes for which such information is transmitted and to maintain its confidentiality;
- participate in discussion groups or *chatrooms on* the Internet concerning financial instruments or issuers of financial instruments, whether listed or unlisted, and in which there is an exchange of information concerning the Group, its companies, competing companies or listed companies in general or financial instruments issued by such entities, unless these are institutional meetings for which a verification of legitimacy has already been carried out by the competent functions or there is no exchange of information whose non-privileged nature is evident;
- leave documents containing Inside Information in places where they could easily be read by people who are not authorized, under company procedures, to know such information;
- disseminate falsified information relating to communications to the market in the event of the issuance of securities.

Furthermore, reference is made to the principles of conduct set out in the*"Sensitive Proceedings in the Area of Corporate Crimes (including Private Bribery Crimes)"*of this Model.

2.8 Sensitive processes in the context of the crimes of manslaughter and serious or very serious bodily harm, committed in violation of accident prevention regulations and the protection of health and hygiene at work

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in art. 25-*seven times of* Legislative Decree 231/01 are the following:

- Management of purchases of goods and services (including consultancy); (Annex C, Sheet 19)
- Selection and management of partner commercial (Annex C, Sheet 02);
- Management of the prevention and protection system for health and safety in the workplace. (Annex C, Sheet 10).

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific category of crimes are identified in Annex C to this Model. Annex C also contains the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph "General control environment", at the beginning of this section,**it is mandatory to** ensure that the aforementioned activities are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in art. 25-*seven times of* Legislative Decree 231/2001 referred to above.

***

The main examples of crimes relating to the following activity are listed below:

- *Management of the prevention and protection system regarding health and safety in the workplace.*

The management of the workplace health and safety prevention and protection system could present risks related to the crimes of manslaughter and serious and very serious personal injury through negligence committed in violation of workplace health and safety regulations. For example, if the Company—in order to achieve cost savings—failed to comply with worker health and safety regulations and caused personal injury to a worker.

With regard to crimes committed in violation of workplace health and safety regulations and environmental crimes, the Company has implemented an internal control system to protect workplace safety. This system aims to prevent potential violations of the relevant legislation and to ensure the technical expertise and powers necessary to verify, assess, and manage risk. This is achieved through the establishment of a suitable organizational structure, internal rules and procedures, and ongoing process monitoring.

In particular, the Company has established its own organizational structure with specific duties and responsibilities in the area of health and safety, formally defined in accordance with the company's organizational and functional framework, from the Employer to the individual worker, with particular attention to the specific roles operating in this area (RSPP – Head of the Prevention and Protection Service, MC – Competent Doctor, RLS – Workers' Safety Representative, ASPP – Prevention and Protection Service Workers, Emergency, First Aid and Fire-Fighting Teams, Supervisors).

In this way, the Company has established its own structure of functions aimed at ensuring the protection of protected interests through the cooperation of multiple entities who, based on the valorization of the necessary differentiated skills, divide the work and share the tasks.

With reference to the activity envisaged above, the specific principles of conduct are indicated below.

Procedures/provisions

- the Company must issue procedures/provisions aimed at formally defining the tasks and responsibilities in terms of safety;
- the Company must monitor workplace accidents and regulate reporting to INAIL in accordance with legal provisions;
- the Company must monitor occupational diseases and regulate the communication of related data to the National Register for Occupational Diseases established at the INAIL database;
- the Company must adopt an internal procedure/provision for organizing preventive and periodic health checks;
- the Company must adopt an internal procedure/provision for the management of first aid, emergencies, evacuations and fire prevention;
- The Company must adopt procedures/provisions for the administrative management of accident and occupational disease claims.

Requirements and skills

- The Head of the Prevention and Protection Service, the competent doctor, the persons in charge of first aid, the persons assigned to the Prevention and Protection Service and the Supervisors must be formally appointed;
- the subjects responsible for monitoring the implementation of maintenance-improvement measures must be identified;

- The doctor must possess one of the qualifications pursuant to art. 38 of Legislative Decree 81/2008, specifically:
- specializing in occupational medicine or preventive medicine for workers and psychotechnics; or
- teaching in occupational medicine or in preventive medicine for workers and psychotechnics or in industrial toxicology or in industrial hygiene or in occupational physiology and hygiene or in occupational clinic; or
- authorization pursuant to Article 55 of Legislative Decree No. 277 of 15 August 1991;
- specialization in hygiene and preventive medicine or in forensic medicine and proven attendance at specific university training courses or proven experience for those who were carrying out the activities of competent doctors on 20 August 2009 or had carried out such activities for at least one year in the previous three years.
- The Head of the Prevention and Protection Service must have professional skills and qualifications in the field of prevention and safety and, specifically, must:
- have a secondary school qualification;
- having participated in specific training courses appropriate to the nature of the risks present in the workplace;
- have obtained a certificate of attendance of specific training courses on risk prevention and protection;
- having attended refresher courses.
- The competent physician must participate in organizing environmental monitoring and receive a copy of the results.

Information

- The Company must provide adequate information to employees and new hires (including temporary workers, interns, and co.co.pro.) regarding the company's specific risks, their consequences, and the prevention and protection measures adopted;
- Evidence must be provided of the information provided for the management of first aid, emergencies, evacuations and fire prevention, and any meetings must be recorded;
- Employees and new hires (including temporary workers, interns, and contract workers) must receive information regarding the appointment of the R.S.P.P. (Head of the Prevention and Protection Service), the company doctor, and the personnel assigned to specific tasks for first aid, rescue, evacuation, and fire prevention;
- information and instructions for the use of work equipment made available to employees must be formally documented;
- the Head of the Prevention and Protection Service and/or the competent doctor must be involved in defining the information programmes;

- the Company must organize periodic meetings between the functions responsible for workplace safety;
- The Company must involve the Workers' Safety Representative in organizing risk detection and assessment activities, and in designating those responsible for fire prevention, first aid, and evacuation activities.

Training

- The Company must provide adequate training to all employees on workplace safety;
- The Head of the Prevention and Protection Service and/or the competent doctor must participate in the drafting of the training plan;
- the training provided must include evaluation questionnaires;
- training must be appropriate to the risks of the task to which the worker is specifically assigned;
- a specific training plan must be prepared for workers exposed to serious and immediate risks;
- Workers who change jobs and those who are transferred must receive preventive, additional, and specific training for their new role;
- the employer, managers and supervisors receive adequate and specific training and periodic refresher courses in relation to their duties in terms of health and safety at work;
- those assigned to specific prevention and protection tasks (fire prevention workers, evacuation workers, first aid workers) must receive specific training;
- The Company must carry out periodic evacuation drills, of which evidence must be provided (a record of the drill carried out with reference to the participants, the progress and the results).

Registers and other documents

- The accident register must always be updated and filled out in its entirety;
- in the event of exposure to carcinogenic or mutagenic agents, a register of those exposed must be drawn up;
- documentary evidence must be provided of the visits to the workplace carried out jointly by the Head of the Prevention and Protection Service and the competent doctor;
- the Company must keep an archive relating to compliance with health and safety requirements at work;
- the risk assessment document may also be kept on electronic media and must be dated or certified by the signature of the employer, as well as, for the sole purpose of proving the date, by the signature of the Head of the Prevention and Protection Service, the RLS or the workers' representative for territorial safety, and the competent doctor;

- the risk assessment document must indicate the criteria, tools and methods used to carry out the risk assessment. The choice of drafting criteria for the document is left to the Employer, who will do so with criteria of simplicity, brevity and comprehensibility, in order to ensure its completeness and suitability as an operational tool for planning company interventions and prevention;
- the risk assessment document must contain the program of maintenance and improvement measures.

Meetings

The Company must organize periodic meetings between the relevant functions, who are permitted to participate in the Supervisory Body, by formally convening the meetings and recording the minutes signed by the participants.

Duties of the Employer and the Manager

- Organize the prevention and protection service - the R.S.P.P. (Head of the Prevention and Protection Service) and the staff - and appoint the competent doctor;
- assess - including in the choice of work equipment, chemical substances or preparations used, as well as in the layout of the workplace - all risks to the health and safety of workers, including those affecting groups of workers exposed to particular risks, including those linked to work-related stress, as well as those connected to differences in gender, age, origin from other countries and the specific type of contract through which the work is performed;
- adapting work to the individual, particularly with regard to the design of workplaces and the choice of equipment and working methods, in particular to reduce monotonous and repetitive work and to reduce the effects of such work on health;
- following this evaluation, prepare a document (to be kept at the company or production unit) containing:
- a report on the assessment of risks to health and safety at work, specifying the criteria adopted for the assessment itself;
- the identification of prevention and protection measures and personal protective equipment, following the assessment in the first point;
- the program of measures deemed appropriate to ensure the improvement of safety levels over time.

  The assessment and drafting of the document must be carried out in collaboration with the Head of the Prevention and Protection Service and the competent physician, after consulting the safety representative. It must be re-performed whenever changes to the production process are significant for worker health and safety, due to technological developments, following significant accidents, or when the results of health surveillance indicate the need for it. In such cases, the risk assessment document must be revised within thirty days of the respective reasons;
- adopt the necessary measures for the safety and health of workers, in particular:

- by designating in advance the workers responsible for implementing fire prevention and fire-fighting measures, for evacuating workers in the event of serious and immediate danger, for rescue, first aid and, in any case, for emergency management;
- identifying the person or persons in charge of carrying out the work of the supervisory activities referred to in art. 19 of Legislative Decree 81/2008;
- updating prevention measures in relation to organizational and production changes that are relevant to health and safety at work, or in relation to the degree of evolution of prevention and protection techniques;
- taking into account the capabilities and conditions of workers in relation to their health and safety, when assigning them the relevant tasks;
- providing workers with the necessary and suitable personal protective equipment, in agreement with the Head of the Prevention and Protection Service;
- by taking appropriate measures to ensure that only workers who have received adequate instructions access areas that expose them to a serious and specific risk;
- requiring individual workers to comply with current regulations, as well as company provisions regarding workplace safety and hygiene and the use of collective protection equipment and personal protective equipment made available to them;
- by sending workers for medical examinations within the deadlines set by the health surveillance program and by requesting the competent doctor to comply with the obligations set by the regulations on workplace safety, informing the doctor of the processes and risks associated with the production activity;
- adopting measures to control risk situations in the event of an emergency and giving instructions so that workers, in the event of serious, immediate and unavoidable danger, abandon their workplace or the danger area;
- informing workers exposed to serious and immediate risks about the risks themselves and the safety specifications adopted;
- refraining, except in duly justified cases, from requiring workers to resume their work in a work situation where a serious and immediate danger persists;
- allowing workers to verify, through the safety representative, the application of safety and health protection measures and allowing the safety representative to access company information and documentation relating to risk assessments, related prevention measures, as well as those relating to dangerous substances and preparations, machinery, systems, work organization and environments, accidents and occupational diseases;
- taking appropriate measures to prevent the technical measures adopted from causing risks to the health of the population or deteriorating the external environment;
- monitoring workplace accidents resulting in absences of at least one day and occupational diseases and maintaining records of the collected data, which must also be kept informed of the prevention and protection service and the competent doctor;

- consulting the safety representative regarding: risk assessment, identification, planning, implementation, and verification of prevention within the Company; the designation of those responsible for prevention services, fire prevention activities, first aid, and worker evacuation; and the organization of training for workers responsible for emergency management;
- adopting the necessary measures for fire prevention and worker evacuation, as well as in the event of serious and immediate danger. These measures must be appropriate to the nature of the activity, the size of the company or production unit, and the number of people present;
- Agree with the competent physician, upon appointment, on the location for storing the health and risk records of the worker undergoing health surveillance, which must be kept in compliance with professional secrecy. A copy of the health and risk records must be delivered to the worker upon termination of the employment relationship, providing the worker with the necessary information regarding the retention of the original. Each affected worker must be informed of the results of the health surveillance and, upon request, receive a copy of the health records.

Workers' Duties

- Observe the provisions and instructions given by the employer, managers and supervisors, for the purposes of collective and individual protection;
- use machinery, equipment, tools, dangerous substances and preparations, means of transport and other work equipment, as well as safety devices correctly;
- use the protective devices made available to them appropriately;
- immediately report to the employer, manager or supervisor any deficiencies in the means and devices referred to in the previous points as well as any other dangerous conditions of which they become aware, taking direct action, in case of emergency, within the scope of their skills and possibilities, to eliminate or reduce such deficiencies or dangers, informing the workers' safety representative;
- do not remove or modify safety, signalling or control devices without authorisation;
- not to carry out on their own initiative operations or maneuvers that are not within their competence or that could compromise their own safety or that of other workers;
- undergo the health checks required of them;
- contribute, together with the employer, managers, and supervisors, to the fulfillment of all obligations imposed by the competent authority or otherwise necessary to protect the safety and health of workers at work.

***

The main examples of crimes relating to the following activities are listed below:

• *Management of purchases of goods and services (including consultancy).*

The management of procurement of goods and services (including consultancy) could present risks related to negligent injury crimes committed in violation of workplace safety regulations, for example, if failure to comply with legal obligations relating to organizational activities (such as procurement management) resulted in injury to a worker.

With reference to the activity described, the specific principles of behavior are indicated below.

Relations with contractors

The Company must prepare and maintain an updated list of companies operating within its sites under a contract.

The management and coordination procedures for contracted work must be formalized in written contracts that specifically reference the obligations set forth in Article 26 of Legislative Decree 81/2008, including, on the part of the employer:

- verify the technical and professional suitability of contracting companies for the work to be awarded, including through registration with the Chamber of Commerce, Industry and Crafts;
- provide detailed information to contractors about the specific risks existing in the environment in which they are intended to operate and about the prevention and emergency measures adopted in relation to their activity;
- cooperate in the implementation of prevention and protection measures against workplace risks affecting the work activity covered by the contract and coordinate protection and prevention measures against risks to which workers are exposed;
- adopt measures aimed at eliminating risks due to interference between the work of the various companies involved in the execution of the overall project.

Except in the case of intellectual services, mere supplies of materials or equipment, as well as works or services whose duration does not exceed two days - provided that they do not involve risks indicated in art. 26 paragraph 3 -*until*Legislative Decree 81/08 - the employer arranges/organizes a joint risk assessment with the contracting companies. The client employer and the contractor must develop a single risk assessment document (DUVRI). which specifies the measures taken to eliminate interference. This document must be attached to the procurement or work contract and must be updated as the work, services, and supplies progress.

In supply, procurement, and subcontracting contracts, costs related to workplace safety must be specifically indicated (which are not subject to discounts). Workers' representatives and trade unions may access this data upon request.

The management of workplace safety obligations in the event of subcontracting must be clearly defined in procurement contracts.

The principal contractor is jointly and severally liable with the contractor, as well as with any further subcontractors, for all damages for which the worker, employed by the contractor or subcontractor, is not compensated by the National Institute for Insurance against Accidents at Work.

In the context of carrying out activities under a contract or subcontracting regime, the client employer requires the contracting or subcontracting employers to expressly indicate the personnel who perform the function of supervisor)

***

The main examples of crimes relating to the following activities are listed below:

- *Selection and management of commercial partners.*

The selection and management of commercial partners could present risk profiles in relation to crimes relating to health and safety at work in the event that, for example, in order to obtain economic savings, the Company selects partner commercial companies that do not comply with the relevant regulations.

For the principles of conduct relating to the "*Selection and management of commercial partners"*, please refer to what is provided in the*"Sensitive Proceedings in Crimes against Public Administration and Crimes of Inducement to Refuse to Make Statements or to Make False Statements to Judicial Authorities"*of this Model.

2.9 Sensitive Processes in the context of environmental crimes

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in art. 25-*eleven times of* Legislative Decree 231/01 are the following:

- *Management of activities with environmental impact*(Annex C, Sheet 21);
- *Management of purchases of goods and services*(including consultancy). (Annex C, Sheet 19).

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are identified in Annex C to this Model. Annex C also contains the internal processes and related company procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph "General control environment", at the beginning of this section,**it is mandatory to** ensure that the aforementioned processes are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in art. 25-*eleven times of* Legislative Decree 231/2001 referred to above.

***

The main examples of crimes relating to the following activities are listed below:

- *Management of activities with environmental impact;*
- *Management of purchases of goods and services (including consultancy).*

The **management of activities with environmental impact may** present risk profiles in relation to the configuration of environmental **crimes**, in the event that, for example, in order to obtain economic advantages, the Company does not equip itself with all the tools necessary to deal with environmental risks.

The **management of purchases of goods and services (including consultancy)**may present risk profiles in relation to the commission of environmental **crimes in** the event that, for example, a subordinate or senior member of the Company were to enter into contracts with unqualified carriers, disposers or intermediaries who do not have the necessary legal authorisations, in order to obtain economic savings for the Company.

To the Recipients as defined above who, by reason of their role or function, are involved in the aforementioned process**it is mandatory**Of:

- be constantly updated on the regulations in force and comply with them;
- identify the nature and characteristics of the waste and assign the correct classification in order to define the correct disposal methods, in accordance with the law;
- enter into contracts with suppliers responsible for the collection and disposal of waste who have the appropriate authorisations and are selected in compliance with the provisions set out in the section "*Management of purchases of goods and services (including consultancy)*" of the "*Sensitive Proceedings in Crimes against Public Administration and Crimes of Inducement to Refuse to Make Statements or to Make False Statements to the Judicial Authority"*Specifically, the aforementioned contracts must contain clauses specifying:
  - that the interested company declares that it respects the principles set out in Legislative Decree 231/2001, as well as adhering to the principles of the Code of Conduct adopted by the Company;
  - that the interested company declares that it has the authorisations required by law to carry out its business;
  - that the untruthfulness of the aforementioned declarations could constitute grounds for termination of this contract pursuant to art. 1456 of the Italian Civil Code.
- provide for the compilation of mandatory documentation, where applicable (registers/forms);

In the context of the aforementioned behaviour it **is forbidden** Of:

- dispose of waste in unauthorized landfills or those that do not have the appropriate permits based on the type of waste;
- using suppliers responsible for waste collection, transport and disposal who do not have the appropriate authorisations;
- dumping hazardous substances in yards, manholes, etc., causing soil/subsoil pollution;
- deposit or abandon waste;
- setting fire to abandoned or uncontrolled waste.

2.10 Sensitive Processes in the context of crimes against the individual personality and crimes related to illegal immigration

The main Sensitive Processes that the Company has identified within itself in relation to the crimes referred to in Articles 25-*quinquies*and 25-*twelve times*of Legislative Decree 231/01 are the following:

- Management of purchases of goods and services (including consultancy); (Annex C, Sheet 19)
- Selection and management of commercial partners; (Annex C, Sheet 2)
- Personnel Management and Reward System; (Annex C, Sheet 11)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are identified in Annex C to this Model. Annex C also contains the internal processes and related company procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory to** ensure that the aforementioned process is carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in Articles 25-*quinquies*and 25-*twelve times*of Legislative Decree 231/2001 referred to above.

***

The main examples of crimes relating to the following activity are listed below:

- *Personnel management and reward system.*

Personnel management could present risks related to the crime of employing third-country nationals whose stay is irregular, for example, if the Company employed foreign workers without a residence permit.

Personnel management could present risks related to the crime of illicit intermediation and labor exploitation if, for example, the Company paid its workers a disproportionately low wage compared to the quantity and quality of the work performed, or repeatedly violated regulations regarding working hours, rest periods, weekly rest, mandatory leave, and holidays.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activity, in addition to what is provided for in the
"Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority" of this Model,**it is mandatory** Of:

- ensure compliance with the regulations relating to working hours, rest periods, weekly rest, mandatory leave and holidays;
- ensure that, during the hiring process, the HR department collects a copy of the candidate's valid residence permit, verifying its expiry date in order to monitor its validity throughout the employment relationship;
- provide the Company with IT tools that prevent access to and/or receipt of material relating to child pornography;
- periodically and unequivocally remind its employees to use the IT tools in their possession correctly.

In the context of the aforementioned behaviors it is prohibited Of:

- Hiring non-EU employees who do not meet the legal requirements to reside and work within the country.

***

The main examples of crimes relating to the following activities are listed below:

- *Management of purchases of goods and services (including consultancy);*
- *Selection and management of commercial partners.*

The management of purchases of goods and services (including consultancy) could present potential risks related to the crime of employing third-country nationals whose stay is irregular, for example, if the Company, as part of a contract, were to turn to suppliers who employ workers who are third-country nationals without a residence permit.

The management of purchases of goods and services (including consultancy) could pose risks related to crimes against individuals if, for example, the Company, as part of a contract, uses suppliers who do not comply with the working conditions required by law.

The selection and management of *partner commercial* activities could present risk profiles in relation to the crime of employing citizens of third countries whose stay is irregular if, for example, the Company, in the context of a contract, turns to third parties who employ workers who are citizens of third countries without a residence permit or who do not comply with the working conditions required by law.

The selection and management of partner/commercial activities could present risk profiles in relation to crimes against the individual personality in the event that, for example, the Company were to turn to partner commercial workers who do not comply with the working conditions required by law.

To the Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of the aforementioned activities, in addition to what is provided for in the*"Sensitive Proceedings in Crimes against Public Administration and Crimes of Inducement to Withhold Statements or to Make False Statements to Judicial Authorities"*of this Model,**it is mandatory** Of:

- ensure the existence of documentation certifying the correct execution of the selection and hiring procedures;
- ensure that the counterparty's compliance with the regulatory requirements for compliance is verified by delivering the documentation required by law (e.g., Single Document of Contribution Regularity – DURC);

For further principles of conduct relating to the "*Management of purchases of goods and services (including consultancy)*" as well as to the "*Selection and management of commercial partners*", please refer to the provisions in the "*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model.

2.11 Sensitive Processes in the context of transnational crimes

The main Sensitive Processes that the Company has identified within itself in relation to certain transnational crimes provided for by Article 10 of Law 146/06 are the following:

- Customer Relationship Management; (Annex C, Sheet 14)
- Management of purchases of goods and services (including consultancy); (Annex C, Sheet 19)
- Selection and management of*partner* commercial; (Annex C, Sheet 02)
- Cash Flow Management; (Annex C, Sheet 15)
- Relationship Management*intercompany;*(Annex C, Sheet 01)
- Management of gifts, donations, events, and sponsorships; (Annex C, Sheet 16)
- Management of activities*remarketing*; (Annex C, Sheet 06)
- Litigation management and relations with the Judicial Authority and management of settlement agreements; (Annex C, Sheet 12)

- Personnel management and reward system. (Annex C, Sheet 11)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are identified in Annex C to this Model. Annex C also contains the internal processes and related company procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions / Departments involved in the Sensitive Processes and reported in Annex C. In addition to what is reported in the paragraph "General control environment", at the beginning of this section,**it is mandatory to** ensure that the aforementioned processes are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In general, **it is forbidden to** engage in behaviors or contribute to the implementation of behaviors that may fall within the categories referred to in art. 10 of Law 146/06 referred to above.

***

For specific principles of conduct in relation to:

- *Customer relationship management;*
- *Management of purchases of goods and services (including consultancy);*
- *Selection and management of commercial partners;*
- *Financial flow management;*
- *Management of intercompany relationships;*
- *Management of gifts, donations, events and sponsorships;*
- *Management of remarketing activities;*
- *Management of development activities.*

please refer to the provisions of the "*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model.

2.12 Sensitive Processes in the field of tax crimes

The main Sensitive Processes that the Company has identified within itself in relation to the tax crimes referred to in art.*25- fifty times of* Legislative Decree 231/01 are the following:

- Customer Relationship Management; (Annex C, Sheet 14)
- Management and assessment of customer credit; (Annex C, Sheet 03)

- Management of purchases of goods and services (including consultancy); (Annex C, Sheet 19)
- Selection and management of commercial partners; (Annex C, Sheet 02)
- Accounting management, budget preparation, and tax management; (Annex C, Sheet 08)
- Management of intercompany relationships; (Annex C, Sheet 01)
- Management of assembly activities, capital transactions and other non-routine operations; (Annex C, Sheet 17)
- Management of internal and external communications (investors, advertising, etc.); (Annex C, Sheet 09)
- Management of remarketing activities; (Annex C, Sheet 06)
- Personnel Management and Reward System; (Annex C, Sheet 11)
- Management of expense reports and entertainment expenses; (Annex C, Sheet 04)
- Management of gifts, sponsorships, and donations. (Annex C, Sheet 16)

The Corporate Functions/Departments involved in the Sensitive Processes listed above and falling within the specific Crime Family are listed in Appendix C to this Model. Appendix C also indicates the internal processes and related corporate procedures.

Specific principles of behavior

The Principles set out below are applicable in general to all Recipients, and in particular, to the Company Functions/Departments involved in the Sensitive Processes and reported in Annex C.

In addition to what is reported in the paragraph “General control environment”, at the beginning of this section,**it is mandatory to** ensure that the aforementioned processes are carried out in full compliance with:

- current laws and regulations;
- *policy* and company and Group procedures;
- principles of loyalty, fairness and clarity;
- Code of Conduct.

In order to manage tax compliance risks and ensure compliance with tax regulations, the Group has implemented a specific tax compliance management procedure that:

- defines the guidelines of the organizational and operational model for managing tax compliance;
- indicates the roles and responsibilities of the organizational units involved in carrying out operational activities;
- identifies the first level controls to be carried out, as well as the related timescales and the evidence that must be archived by each process *owner*.

In general, **it is forbidden to** carry out behaviors or contribute to the carrying out of behaviors that may fall within the categories referred to in Article 25*fifty times of* Legislative Decree 231/2001 referred to above.

***

The main examples of crimes in relation to the following processes are listed below:

- *Customer relationship management;*
- *Management of remarketing activities;*
- *Management and assessment of customer credit.*

Managing commercial relationships with customers could present risks related to the configuration of tax crimes if, for example, the Company issues fictitious credit notes for the purpose of evading income and value added taxes.

The management of commercial relationships could present risks related to the crime of issuing invoices or other documents for non-existent transactions, for example, if invoices were issued or released to third parties to allow them to evade income or value added taxes, in exchange for sales that were in fact fictitious or not executed in whole or in part.

The management of remarketing activities could present risks related to the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions, for example, if a senior executive or subordinate of the Company enters into contracts for the sale of used vehicles as part of non-existent transactions.

The management of remarketing activities could present risks related to the configuration of tax crimes in the event that, for example, the Company issues invoices for non-existent transactions with the aim of evading income and value added taxes by a third party.

The management and assessment of customer credit may present risks related to the crime of fraudulent misrepresentation through other means, for example, if a subordinate or senior executive of the Company, based on documents representing a false accounting record, writes down the credit or charges losses on credit even in the absence of the requirements established by the law.

In order to identify **the principles of behavior in the management of commercial relationships with customers, the management of marketing activities *remarketing and customer credit management and assessment activities***, please refer to the provisions of:

- "*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model and the main principles of conduct are reported below:

- ensure, where necessary, that customer relationships are managed exclusively by persons with appropriate powers;
- ensure compliance with all provisions of the Group's policies and procedures, particularly those relating to anti-money laundering, antitrust and conflict of interest;
- ensure the traceability of all phases of the commercial process, including the definition of financial conditions, any discounts applied, and the duration of agreements, through the use of the required information systems;
- provide for adequate segregation of tasks and responsibilities in customer management, with particular reference to the definition of financial conditions and payment methods and times;
- ensure that commercial offers/proposals are defined on the basis of company procedures;
- ensure that relationships with customers are formalized in specific written agreements (commercial offers/proposals), approved by persons with specific powers;
- ensure that preliminary screening is carried out on new clients, both in terms of compliance, including anti-money laundering, and creditworthiness;
- ensure the segregation of duties in all phases relating to customer relationship management and remarketing activities, including the creation of customer databases;
- ensure that any exceptions to the economic conditions, determined automatically through the use of a specific system, are authorised in compliance with the system of delegations and procedures;
- ensure the traceability of all phases of the sales entity agreement process;
- carry out specific verification activities related to credit management;
- evaluate customer credits by using credit management systems*rating;*
- ensure that credits are written off only on the basis of internal policies and procedures, reliable and reliable documentation certifying the actual irrecoverability of the credit, and in accordance with accounting principles and tax regulations;
- ensure the traceability of all documentation sent to customers;
- verify the regularity of invoicing towards customers;
- carry out a specific analysis of complaints received from customers;
- forward the financing application to the competent signature level for the approval;
- in the event that the services provided to customers are carried out - in whole or in part - with the support of third parties, ensure that their selection always takes

place in compliance with the provisions set out in the "Selection and Management of Commercial Partners" section of this chapter;

- communicate, without delay, to *management companies* and, at the same time, the Supervisory Body, any critical issues that may arise within the processes under examination.

- *"Sensitive Trials in the context of the crimes of receiving stolen goods, money laundering, and use of money, goods, or utilities of illicit origin, as well as self-laundering, organized crime offenses, and crimes with the aim of terrorism or subversion of the democratic order."*and the main principles of behavior are reported below:

  - identify and understand the customers and the individuals on whose behalf the customers operate (so-called beneficial owners);
  - identify the beneficial owner(s) of the legal entity customer in accordance with the procedures established by the relevant legislation;
  - ensure that customer due diligence is carried out on its counterparties and assign a consistent money laundering and terrorist financing risk profile;
  - proceed to verify the documentation, data or information obtained;
  - verify the accuracy and completeness of the personal data and information relating to the economic activity carried out;
  - verify the consistency between the person(s) included in the financing request as beneficial owner(s) and what appears in the tool computer scientists;
  - ensure that all documentation relating to customer identification activities as well as periodic checks carried out on customer positions is adequately archived by the relevant bodies;

To the Recipients as defined above who, by reason of their role or function, are involved in the management of the aforementioned processes,**it is also mandatory** Of:

- ensure that the recipient of the invoice coincides with the contractual counterparty identified when creating the master data;
- ensure adequate segregation of duties and responsibilities for all phases of the active cycle (management of administrative and accounting obligations relating to customer invoicing, invoice recording, collection management, etc.);
- perform a consistency check between the invoice recipient, identified based on the contractual provisions recorded in the system, and the person who made the payment;
- ensure that proceeds are received via bank transfer and that they are always traceable and verifiable.

- ensure that the transfer of credits to write-offs is authorised by previously identified persons, in line with the system of delegations and powers of attorney adopted by the Company;
- refrain from carrying out transactions that are, in whole or in part, simulated or otherwise fraudulent.

In the context of the aforementioned behaviour it **is forbidden to:**

- enter into contracts with prices and conditions established according to non-objective parameters and/or in violation of the provisions of company procedures and relevant legislation;
- issue invoices or other documents relating to transactions that are wholly or partially non-existent;
- accept requests for contributions in cash and/or from parties other than those indicated in the accounting documentation.
- authorize the transfer to loss of credits without the requirements being met.

***

The main examples of crimes in relation to the following process are listed below:

- *Management of purchases of goods and services (including consultancy).*

The management of purchases of goods and services (including consultancy) could present risks in relation to the configuration of tax crimes if, for example, the Company records invoices relating to the purchase of a good or service in the context of transactions that are wholly or partially non-existent.

The management of purchases of goods and services (including consultancy) could present a risk for the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions. For example, if invoices or other documents for objectively non-existent transactions were recorded in the registers and subsequently reported in IRES/IRPEF or VAT returns—for the purpose of evading value added tax and income tax—because they never occurred or indicated amounts higher than the actual value (so-called over-invoicing).

The management of purchases of goods and services (including consultancy) could present risks for the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions. For example, if invoices or other documents for transactions that actually occurred were recorded in the registers and subsequently reported in tax returns—for the purpose of tax evasion—but between parties other than those indicated in the accounting documentation and who actually provided the service (so-called subjectively non-existent transactions).

In order to identify **the principles of behavior in the management of purchases of goods and services (including consultancy)**, please refer to the provisions of the "*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to*

make statements or to make false statements to the Judicial Authority" of this Model and the main principles of conduct are reported below:

- create a specific supplier registry to collect and record all critical and significant information about them;
- subject suppliers to a qualification process that allows for the verification of their financial soundness, commercial, technical-professional and ethical reliability;
- ensure that the selection of suppliers and consultants takes place among the names selected on the basis of criteria identified within the internal regulations, without prejudice to occasional needs/supplies
- ensure compliance with the *iter* approval of suppliers and contracts, as required by company procedures;
- ensure adequate segregation of functions in the supplier/consultant selection process;

  proceed, in accordance with company procedures, to select the supplier by comparing three offers, except in special cases which must be duly justified (such as: low-value contracts, intra-group agreements, contracts with specific companies, a relationship of trust established with the consultant or supplier, etc.);
- verify the existence of specific authorizations of suppliers who carry out activities for which they are required;
- verify, during the qualification phase and periodically, the possible presence of Suppliers in the*Black List*;
- ensure traceability, including through specific information systems, of the *iter* supplier selection, qualification and evaluation, through the formalization and archiving of the relevant supporting documentation, in the manner established by company procedures and the IT tools supporting the process;
- ensure that all payments to suppliers are made if adequately supported by contract or order, only following validation according to the *iter* predefined internal authorization and after having verified the compliance of the products with what was ordered;
- ensure that all relationships with suppliers or consultants are formalized within specific written agreements approved according to the system of delegations and powers of attorney and where the price of the goods or the consideration for the service is clearly defined;
- ensure that contracts stipulated with suppliers/consultants specifically provide for: object of the contract, agreed compensation, payment method, ethical and contractual clauses *compliance*, termination clauses or alternatively verify that the contractual conditions proposed by third parties provide for compliance with the principles set out in Legislative Decree 231/01, as well as ethical ones;
- ensure the traceability and retrospective reconstructability of commercial transactions through the formalization and archiving, including through specific information systems, of the relevant supporting documentation;

- ensure periodic monitoring, through the use of specific tools, of the suppliers' performance, as well as use the results of these assessments for the purposes of their qualification;
- carefully investigate and report to the Supervisory Body:
  - o requests for unusually high commissions;
  - o requests for expense reimbursements that are not adequately documented or are unusual for the operation in question.

To the Recipients as defined above who, by reason of their role or function or mandate, are involved in the aforementioned activity it **is also mandatory to:**

- ensure that supplier records can only be modified following a predefined procedure, by previously identified parties with the necessary authorization powers regarding the purchase of goods and services;
- ensure appropriate checks are carried out on the supplier's history, as well as the adequacy of its financial, personnel and warehouse structure with respect to the supply activity;
- verify the regularity of payments with reference to the full correspondence of the recipients/orderers and the counterparties actually involved in the transaction, in particular, it must be precisely verified that there is correspondence between the person to whom the order is made out and the person who collects the related sums;
- carry out specific checks regarding the ownership of suppliers' current accounts and duly justify situations in which financial flows are not disbursed:
  - in the country of residence of the supplier and/or the Company;
  - in the country where the supply takes place.
- monitor the consistency between what was ordered and what was received as well as the conformity of the services performed by consultants and suppliers with respect to what was contractually established;

In the context of the aforementioned behaviour it **is forbidden** Of:

- proceed with the recording in the accounting and the subsequent indication in the tax returns of invoices or other documents received in the context of non-existent transactions (in whole or in part);
- make payments in cash, to numbered current accounts or accounts not in the name of the supplier or other than those provided for in the contract;
- make payments in countries other than the supplier's country of residence;
- make payments that are not adequately documented and/or not authorized in accordance with the provisions of the delegation and power of attorney system;
- bind the Company with verbal orders/contracts or those without a clear definition of the goods/services to be received and the price of the goods or the consideration for the service;

- provide services to consultants and suppliers that are not adequately justified within the contractual relationship established with them and pay them compensation that is not adequately justified in relation to the type of assignment to be performed and current local practices;
- make payments to an account other than the one indicated in the account details or to credit institutions based in tax havens or which do not have physical locations in any country.

***

The main examples of crimes in relation to the following process are listed below:

- *Personnel management and reward system.*

Personnel management activities could present risks related to the crime of fraudulent tax returns through other means if, in order to evade income taxes, a Company employee were granted a lower salary than that indicated in the certified statement used to deduct the related cost, and, consequently, the legal representative indicated fictitious liabilities in the tax return.

Personnel management could present risks related to the crime of fraudulent tax returns through the use of invoices or other documents for non-existent transactions. For example, if pay slips and expense reports referring to non-existent individuals or indicating higher amounts than the actual ones were used, the legal representative consequently indicated fictitious liabilities in the tax return.

In order to identify **the principles of behavior in the context of personnel management and reward system**, please refer to the provisions of the "*Sensitive processes in crimes against the Public Administration: crimes of inducing not to make statements or to make false statements to the Judicial Authority*" of this Model and the main principles of conduct are reported below:

- hire staff only and exclusively with a regular employment contract and with remuneration consistent with the applicable Collective Bargaining Agreement;
- ensure the archiving of the remuneration surveys periodically conducted by the Company;
- ensure that the contracts are signed by persons with appropriate powers;
- ensure that the incentive system is consistent with the Group's remuneration policy
- ensure that any incentive systems correspond to realistic objectives and are consistent with the tasks, activities performed and responsibilities assigned;
- ensure the traceability of the incentive process, through the formalization of objectives and the related reporting.

***

The following is a list of the main examples of crimes in relation to the following process:

- *Selection and management of commercial partners.*

Managing relationships with business partners could present risks related to the commission of tax crimes if, for example, a senior or subordinate individual, in order to obtain an illicit tax advantage for the Company, were to record invoices in the accounting records for transactions that were wholly or partially non-existent.

In order to identify **the principles of behavior in the selection and management of business *partners***, please refer to the provisions of the "*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model and the main principles of conduct are reported below:

- ensure that the selection and qualification process of partner/commercial transactions always take place in full compliance with the provisions of company procedures*;*
- ensure an adequate process of due *diligence* of any*partner*commercial which includes, among other things, the verification of the commercial and professional reliability and the integrity requirements of the counterparties;
- verify, during the qualification phase and periodically, the possible presence of *partner* in the *Black List*;
- verify the identity of the counterparty;
- ensure the traceability of the *iter* of selection;
- respect the principles of transparency, professionalism, reliability, motivation and non-discrimination in the choice of the counterparty;
- ensure that the agreed fees fall within normal market conditions and are in any case contractually defined on the basis of objective calculation criteria;
- ensure that the contractual mechanism used contains specific information on the rules of conduct adopted by the Company with reference to Legislative Decree 231/2001 and on the consequences that behaviors contrary to the provisions of the Code of Conduct and current legislation may have with regard to contractual relationships;
- ensure that the assignment of the mandate to the counterparty is evidenced by a written document;
- Disburse fees transparently, always documentable, and reconstructable after the fact. In particular, verify the correspondence between the recipient of the payment and the provider of the service;
- submit the *partner* qualified for checks and *audit periodicals* as required by company procedures.

In the context of the aforementioned behaviors**it is forbidden** Of:

- bind the Company with verbal contracts with the counterparty;

- issue or accept invoices for non-existent transactions;
- make payments and reimburse expenses to counterparties that are not adequately justified in relation to the type of business performed, are not supported by fiscally valid receipts, and are not shown on the invoice;
- certify the receipt of non-existent commercial services;
- create extra-accounting equity funds for transactions contracted at above-market conditions or for invoices that are non-existent in whole or in part.

***

The following is a list of the main examples of crimes in relation to the following process:

- *Management of expense reports and entertainment expenses.*

For example, expense management could pose a risk of fraudulent tax returns using documents for non-existent transactions if, in order to evade income tax or VAT, expense reports were issued for expenses not incurred (in whole or in part), and the legal representative subsequently indicated fictitious liabilities in the tax return relating to those taxes.

In order to **identify the principles of conduct in the management of expense reports and entertainment expenses**, please refer to what is provided in the*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model and the main principles of conduct are reported below:

- prepare expense reports in compliance with company procedures, using dedicated company IT tools;
- ensure that expense claims are reimbursed only after they have been approved by appropriately authorized persons, based on a segregated process, and only in the presence of proper supporting documents;
- carry out specific checks and monitoring regarding the use of company credit cards and, more generally, employee expense reports;
- ensure compliance with the internal limitations defined by company procedures regarding expense reports and the use of company credit cards, as well as regarding entertainment expenses;
- verify that the expenses incurred are related to the performance of the work activity, appropriate and adequately documented by attaching fiscally valid receipts;
- ensure that entertainment expenses are not repetitive for the same beneficiary and that full traceability of the participating entities is guaranteed;
- ensure a periodic verification process of staff expense reports;

- ensure that, in the event of abnormal expenses, they are not reimbursed;
- communicate, without delay, to their hierarchical manager or to the Company's management and at the same time to the Supervisory Body any behavior aimed at obtaining an illicit advantage for the Company.

In the context of the aforementioned behaviour it **is forbidden** Of:

- make expense reimbursements that:
  - have not been duly authorized;
  - do not find adequate justification in relation to the type of activity carried out;
  - are not supported by fiscally valid documents or are not shown in the notes.

The following is a list of the main examples of crimes in relation to the following process:

- *Management of intercompany relationships*

For example, the management of intercompany relationships could present risks related to the crime of fraudulent tax returns through the use of invoices for non-existent transactions, if, in order to evade taxes, it were possible to receive invoices from group companies for services not rendered (in whole or in part), or if invoices were used for services rendered between parties other than those shown in the accounting documentation, and, consequently, the legal representative indicated fictitious liabilities in the tax return relating to such taxes.

In order to **identify the principles of behavior in the management of intercompany relationships,**please refer to what is provided in the*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model and the main principles of conduct are reported below:

- ensure that relationships *intercompany* are regulated by specific contracts/agreements governing, among other things, roles, responsibilities and agreed compensation;
- ensure the correct and complete preparation, in line with the provisions of applicable legislation, of transfer pricing documentation, suitable for certifying the conformity of the transfer prices applied in intragroup transactions with the "normal value";
- ensure that the above documentation contains, among other things, the following information:
  - mapping of intra-group transactions;
  - the definition of cost-sharing agreements;
  - the formulation of a transfer pricing policy;
- ensure that the documentation is signed by persons with appropriate powers;
- ensure that documentation is archived at the functions involved in the process;

- communicate, without delay, to *management companies* and, at the same time, the Supervisory Body, any critical issues that may arise within the scope of the activity in question.

The Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the management of intercompany relationships are obliged **to:**

- refrain from carrying out transactions that are, in whole or in part, simulated or otherwise fraudulent;
- retain proof of the effectiveness of the services provided;
- verify the actual execution of the service, the consistency of the execution methods adopted with the regulatory requirements applicable from time to time and the compatibility of the conditions applied with the generally accepted criteria for determining the normal value of transactions.

In the context of the aforementioned behaviour it **is forbidden** Of:

- record invoices or keep documentation for services that are, in whole or in part, non-existent;
- destroy or conceal accounting records or other relevant documentation in order to obtain a tax advantage;
- carry out transactions with Group companies, in order to evade tax regulations.

***

The main examples of crimes in relation to the following process are listed below:

- *Accounting management, budget preparation and tax management*

Accounting, financial statement preparation, and tax management could pose potential risks related to the crime of fraudulent tax returns through the use of invoices or other documents for non-existent transactions, should the Company record invoices in its accounts for (wholly or partially) non-existent transactions, with the aim of evading income or value added taxes.

Accounting, financial statement preparation, and tax management could pose potential risks related to the crime of fraudulent tax returns through other means, if the Company includes simulated items in its financial statements, supported by false documentation, in order to be able to report fictitious liabilities or assets that are lower than the actual ones.

Accounting management could present risks related to the crime of concealment or destruction of accounting documents if, for example, the Company's legal representative, in order to evade income and value added tax, concealed or destroyed mandatory documents, thus preventing the tax authorities from reconstructing the Company's income and turnover.

Tax management, and therefore the management of tax returns, could present potential risks in relation to the crime of fraudulent tax returns through the use of invoices or other documents

for non-existent transactions, and fraudulent tax returns through other means. For example, if the Company were to indicate, in its tax/VAT return, fictitious information based on false invoices or other documents issued for non-existent transactions, recorded in the mandatory accounting records, or otherwise held as evidence against the Tax Authorities.

In order to identify **the principles of behavior in the field of accounting management, budget preparation and tax management** please refer to the provisions of the "*Sensitive Processes in the context of corporate crimes (including corruption crimes between private individuals)"*of this Model and the main principles of conduct are reported below:

- maintain correct, transparent, and collaborative behavior, in compliance with the law, applicable accounting principles, and internal rules, in all activities aimed at preparing the financial statements and other corporate communications, in order to provide truthful and accurate information on the Company's economic, financial, and fiscal situation;
- ensure the strictest accounting transparency at all times and under any circumstances;
- clearly and completely identify the functions affected by the communications, as well as the data and information that they must provide;
- ensure the necessary training on the main legal and accounting concepts and issues relating to the financial statement, aimed at the managers of the functions involved in the preparation of the financial statement and other related documents, taking care, in particular, both of the training of new hires and of the carrying out of periodic refresher courses
- observe the rules of clear, correct and complete recording in the accounting activity of facts relating to the management of the Company;
- ensure the completeness and accuracy of accounting closings;
- ensure compliance with company rules relating to the preparation of statutory and consolidated financial statements;
- ensure compliance with the rules of segregation of duties between the person who carried out the operation, the person responsible for recording it in the accounts and the person carrying out the related control;
- proceed with the evaluation and recording of economic and patrimonial elements in compliance with the criteria of reasonableness and prudence, clearly illustrating, in the relevant documentation, the criteria that guided the determination of the value of the asset;
- ensure the correct application of accounting principles for the definition of civil law balance sheet items and a correct operating method for their accounting;
- ensure that transactions and accounting records are documented in order to be able to reconstruct, with a reasonable level of detail, that the accounting records reflect the transactions that occurred;
- provide for the use of systems that guarantee the integrity of accounting records and the traceability of the activities carried out on them;

- ensure compliance with obligations (both in terms of tax returns and payments) and deadlines set by tax legislation;
- ensure that major regulatory developments in tax matters are promptly disseminated to personnel involved in tax management;
- ensure that the draft budget is subject to verification by all company functions required by company procedures;
- to base relations with the Supervisory Authorities, including the tax authorities, on maximum transparency, collaboration, availability and in full compliance with the institutional role played by them and with the existing legal provisions on the matter, the general principles and rules of conduct referred to in the Code of Conduct as well as in this part of the Model;
- use accounting systems that guarantee the traceability of individual transactions and the identification of users who enter data into the system or modify its contents;
- ensure compliance with the requirements of the legislation on direct and indirect taxes;
- ensure the proper functioning of the Company and its corporate bodies, guaranteeing and facilitating all forms of internal control over corporate management required by law, as well as the free and correct formation of the assembly's will;
- assign consultancy tasks having as their object activities other than accounting auditing to the auditing firm or to the companies or professional entities belonging to the same *network* of the auditing firm, exclusively in compliance with current legislation;
- Where third parties (companies, consultants, professionals, etc.) are used to manage activities, ensure that relationships with them are formalized through written contracts containing clauses specifying:
    - that the third party declares that it respects the principles set out in Legislative Decree 231/2001, as well as adhering to the principles of the company Code of Conduct;
    - that the third party declares that it has implemented all necessary measures and precautions aimed at preventing the crimes indicated above, having equipped its corporate structure – where possible – with internal procedures and systems that are fully adequate for such prevention;
    - that the untruthfulness of the aforementioned declarations could constitute grounds for termination of the contract pursuant to art. 1456 of the Italian Civil Code;
- Report to their line manager or company management and, at the same time, to the Supervisory Body, both the existence of errors or omissions in the accounting process of management events and behaviors that do not comply with the above provisions.

The Recipients as defined above who, by reason of their role or function or specific mandate, are involved in the aforementioned process are obliged **to:**

- maintain correct, transparent, and collaborative behavior, in compliance with the law, in all activities aimed at accounting records, including those relevant for tax purposes, as well as fulfilling obligations under tax legislation;

- carry out all obligations promptly, correctly, and in good faith, including the transmission of declarations and communications, as well as the liquidation and payment of taxes and duties, in compliance with the deadlines set by the tax legislation in force from time to time;
- correctly record each transaction, verifying that it is duly authorized, verifiable, legitimate, consistent and appropriate;
- ensure adequate segregation of duties and responsibilities in all phases of managing compliance with tax regulations regarding direct taxes and VAT;
- provide for the analysis of tax risks, in relation to the evolution of the activities carried out by the Company, to changes in the regulatory framework or to particularly significant legal rulings;
- ensure that specific periodic checks are carried out regarding:
    - the timely and correct compliance with the deadlines within which the obligations for submitting tax returns and communications, as well as for paying taxes, duties, contributions and withholdings must be fulfilled;
    - the truthfulness of the declarations in relation to the accounting records;
    - the correctness of the taxes paid;
    - the correspondence between the amounts of taxes paid and the amounts actually paid;
- ensure that all documents supporting registrations, tax declarations, and communications are accurate, verified, authorized, and retained for the periods established by current legislation, in an orderly fashion and in such a way that checks can be carried out at any time;
- Maintain accounting records and other documents that must be kept for tax purposes in a correct and orderly manner, including by implementing physical and/or IT defenses to prevent destruction or concealment.

In the context of the aforementioned behaviors it is **prohibited** Of:

- carry out actions aimed at providing misleading information with reference to the actual representation of the Company, failing to provide a correct representation of the economic, patrimonial, financial and tax situation of the Company;
- carry out transactions, including with Group companies, in order to evade tax regulations;
- create, or allow to be created, illicit, hidden or otherwise incorrectly accounted funds, through any illicit, simulated, fictitious and/or incorrectly accounted financial operation or movement;
- record invoices or keep documentation for services that are, in whole or in part, non-existent;
- destroy or conceal accounting records or other relevant documentation in order to obtain a tax advantage;

- prepare or contribute to the preparation of documents that are completely or partially false in order to obtain undue advantages, for example to justify accounting records aimed at obtaining undue tax benefits;
- engage in misleading conduct that could lead the Board of Statutory Auditors or the auditing firm to make technical or economic errors in the assessment of the documentation presented;
- engage in behaviors that materially impede, through the concealment of documents or the use of other fraudulent means, or that in any case hinder the performance of the audit activity by the statutory audit firm;
- alter or destroy financial and accounting documents and information available online through unauthorized access or other actions suitable for the purpose;
- submitting false statements to the Supervisory Authorities, exhibiting documents that do not correspond in whole or in part to reality.

***

The main examples of crimes in relation to the following process are listed below:

- *Management of assembly activities, capital transactions and other non-routine operations*

The management of capital transactions and other non-routine operations could present risks related to tax crimes if, for example, the Company were to carry out covert transactions or transactions involving inconsistent values, rendering the assets non-existent.

The management of capital transactions and other non-routine operations could present risks related to tax crimes if, for example, the sale of shareholdings or the write-down of shareholdings were simulated.

In order to identify **the principles of conduct in the management of assembly activities, capital transactions and other non-routine operations**Please refer to the provisions of "Sensitive Processes in the context of corporate crimes (including corruption between private individuals)". The main principles of conduct are also reported here.

Capital and/or non-routine transactions are resolved and approved by the Board of Directors and/or the Shareholders' Meeting.

All documentation must be archived by the functions involved in the process in accordance with company rules and applicable legislation.

With regard to the management of assembly activities, capital transactions, and other non-routine operations, the parties involved must ensure the proper functioning of the Company and its corporate bodies, guaranteeing and facilitating the free and correct formation of the assembly's will.

The Recipients as defined above who, by reason of their role or function or mandate, are involved in the management of assembly activities, capital transactions and other non-routine transactions are required to obligation Of:

- ensure compliance with the rules on segregation of duties among the parties involved in managing assembly activities, capital transactions and other non-routine operations;
- ensure that administrative and accounting requirements relating to capital transactions and other non-routine transactions are managed with the utmost diligence and professionalism, avoiding conflicts of interest;
- ensure that the exclusive power to decide on the completion of transactions such as (for example): purchases, sales, mergers, investments, divestments or assumption of commitments in general by the Bank and its directly or indirectly controlled companies of strategic importance, is vested - within the limits set by the Articles of Association - in the Board of Directors;
- ensure the proper functioning of the corporate bodies by allowing for any internal controls;
- make available data and documents requested by the supervisory bodies in a timely manner and in clear, objective and comprehensive language in order to provide accurate, complete, truthful and truthful information.

With reference to extraordinary financial transactions (typically referring to the issuance of bonds, the assumption of loans and financing, the subscription and increases in share capital, the granting of guarantees and sureties, the granting of financing and the subscription of bonds, the acquisition of business units or shareholdings, and other extraordinary transactions such as mergers, demergers, and contributions), the parties involved must ensure that: the competent body, be it the Board of Directors or another formally delegated person, has adequate information support to be able to make an informed decision.

For each extraordinary financial transaction to be approved, the delegated function is required to prepare documentation suitable for assessing its feasibility and strategic and economic suitability, including, where applicable:

- qualitative and quantitative description of the target (feasibility study, financial analysis, studies and statistics on the reference market, comparisons between different alternatives for carrying out the operation);
- characteristics and subjects involved in the operation, also through analysis of *compliance* on the same;
- technical structure, main guarantees and collateral agreements and financial coverage of the operation;
- methods for determining the economic conditions of the operation and indication of any external consultants/intermediaries/advisors involved;
- impact on the prospective economic, financial and equity situation;
- assessments regarding the appropriateness and compliance of the transaction to be approved with the Company's interests.

The Recipients as defined above who, by reason of their role or function or mandate, are involved in the management of capital operations and other non-routine operations, are also obliged **to:**

- ensure adequate process segregation in all phases of the Bank's capital and/or non-routine operations, involving internal functions as well as, where necessary, an expert consultant specializing in tax matters
- ensure the preventive assessment of any tax risks and compliance with tax legislation;
- Ensure the adequacy of all supporting documentation so that the Board of Directors can assess the feasibility and strategic and economic viability, as well as the tax risks, of each transaction. In this regard, the information support may also include one or more tax opinions.

In the context of behaviors it is **prohibited** Of:

- carrying out, during meetings, simulated or fraudulent acts aimed at altering the regular process of forming the assembly's will;
- carry out actions aimed at providing misleading information with reference to the actual representation of the Company, failing to provide a correct representation of the economic, patrimonial, financial and tax situation of the Company;
- omit data and information required by law on the economic, patrimonial and financial situation of the Company;
- carry out transactions in order to evade tax regulations;
- proceed with the fictitious formation or increase of share capital by: (i) attribution of shares or quotas in an amount that is overall greater than the amount of the share capital, (ii) reciprocal subscription of shares or quotas, (iii) significant overvaluation of contributions of assets in kind or credits or of the Bank's assets in the event of transformation;
- engage in misleading conduct that could lead the Board of Statutory Auditors or the Auditing Firm to make an error in the technical-economic evaluation of the documentation presented;
- present incomplete documents and false or altered data.

***

The following is a list of the main examples of crimes in relation to the following process:

- *Management of gifts, donations, events and sponsorships.*

The management of gifts, donations, events, and sponsorships could present risks related to the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions. For example, if it were possible to record in the registers and subsequently include in the IRES/IRPEF or VAT returns—for the purpose of evading VAT and

income tax—documents relating to sponsorships that were not carried out in whole or in part, or whose value is clearly abnormal compared to the market value, these documents relate to sponsorships that were not carried out in whole or in part, or whose value is clearly abnormal compared to the market value.

In order to identify **the principles of conduct in the management of gifts, donations, events and sponsorships please** refer to the provisions of the "*Sensitive Proceedings in crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority*" of this Model and the main principles of conduct are reported below:

- ensure compliance with company and group rules governing the processes listed above;
- ensure that all events are approved according to the current delegation scheme;
- in the case of events organised by the Company with the support of third parties (agencies, organisers, etc.), ensure that the selection of the same always takes place in compliance with the provisions set out in the section "*Management of purchases of goods and services (including consultancy)*" of this chapter;
- ensure that gifts are of reasonable value, tied to a predefined commercial purpose and purchased and provided in compliance with company procedures;
- ensure the existence of a catalogue of goods/services that can be given away free of charge, with an indication of the cost of each item;
- validate any freebies not included in the catalogue;
- ensure the transparency and traceability of the approval and distribution process for free gifts;
- ensure the complete and correct archiving and recording, including through dedicated registers, of the freebies provided, indicating, among other things, the characteristics of the individual gadgets and the relevant recipients;
- ensure that donations and acts of generosity are approved by persons with appropriate powers;
- to foresee one screening of the hypothetical beneficiary of the donation, for the purposes of verifying the specific characteristics and integrity of the same;
- ensure the transparency and traceability of donations and charitable acts made;
- ensure that the documentation certifying the contribution disbursed is fully archived by the functions involved;
- ensure that relationships with counterparties are formalized through appropriate contractual instruments;

In the context of the aforementioned behaviour it **is forbidden** Of:

- proceed with the signing of contracts in the context of operations that (in whole or in part) do not exist;

- proceed with the recording in the accounting and the subsequent indication in the tax returns of documents received in the context of non-existent transactions (in whole or in part);
- make payments in cash, to numbered current accounts or to parties other than those indicated in the contractual instruments;
- making donations and acts of generosity that are not adequately authorised, formalised and accounted for.

ANNEX A: The types of predicate crimes

1. **The types of crimes against the Public Administration (articles 24 and 25 of Legislative Decree 231/01)**

Art. 24

Improper receipt of funds, fraud against the State, a public body, or the European Union, or fraud to obtain public funds, computer fraud against the State or a public body, and fraud in public procurement.

1. *In relation to the commission of the crimes referred to in Articles 316-bis, 316-ter, 353, 353 bis*, 356,*640, paragraph 2, no. 1, 640-bis and 640-ter if committed to the detriment of the State or another public entity or the European Union, of the Criminal Code, a pecuniary sanction of up to five hundred quotas applies to the entity.*
2. *If, following the commission of the crimes referred to in paragraph 1, the entity has obtained a significant profit or has suffered particularly serious damage, a pecuniary sanction of between two hundred and six hundred shares shall apply.*

2-bis. The sanctions provided for in the preceding paragraphs in relation to the commission of the crime referred to in Article 2 of Law No. 898 of 23 December 1986 shall apply to the entity.

3. *In the cases provided for in the previous paragraphs, the interdictory sanctions provided for in Article 9, paragraph 2, letters c), d) and e) shall apply.*

Art. 25

Embezzlement, misappropriation of money or movable property, extortion, undue inducement to give or promise benefits, corruption.

1. *In relation to the commission of the crimes referred to in Articles 318, 321, 322, paragraphs one and three, and 346-bis of the Criminal Code, a fine of up to two hundred quotas applies. The same fine applies, when the act harms the financial interests of the European Union, in relation to the commission of the crimes referred to in Articles 314, paragraph one, 314-bis, and 316 of the Criminal Code.*
2. *In relation to the commission of the crimes referred to in Articles 319, 319-ter, paragraph 1, 321, 322, paragraphs 2 and 4, of the Criminal Code, the entity is subject to a pecuniary sanction of between two hundred and six hundred shares.*
3. *In relation to the commission of the crimes referred to in Articles 317, 319, aggravated pursuant to Article 319-bis when the entity has obtained a significant profit from the act, 319-ter, paragraph 2, 319-quater and 321 of the Criminal Code, the entity shall be subject to a pecuniary sanction ranging from three hundred to eight hundred shares.*
4. *The pecuniary sanctions provided for the crimes referred to in paragraphs 1 to 3 apply to the entity even when such crimes were committed by the persons indicated in Articles 320 and 322-bis.*
5. *In cases of conviction for one of the crimes indicated in paragraphs 2 and 3, the disqualification sanctions provided for in Article 9, paragraph 2, shall apply for a period of not less than four years and not more than seven years, if the crime was committed by one of the persons referred to in Article 5, paragraph 1, letter a), and for a period of not*

less than two years and not more than four, if the crime was committed by one of the persons referred to in Article 5, paragraph 1, letter b).

5-bis. *If, prior to the first-instance ruling, the entity has effectively taken steps to prevent the criminal activity from leading to further consequences, to secure evidence of the crimes and to identify those responsible, or to seize the sums or other assets transferred, and has eliminated the organizational deficiencies that led to the crime by adopting and implementing organizational models suitable for preventing crimes of the type that occurred, the prohibitory sanctions shall have the duration established in Article 13, paragraph 2.*

The individual cases covered by Legislative Decree 231/01 in Articles 24 and 25 are briefly described below.

- ***Embezzlement (art. 314, paragraph 1, of the Criminal Code)***

This type of crime occurs when a public official or person in charge of a public service, having by virtue of his office or service the possession or in any case the availability of money or other movable property belonging to others, appropriates it.

The crime may lead to the administrative liability of the Entity when the act harms the financial interests of the European Union.

- **Improper use of money or movable property (art. 314)*until* c.p.)**

This crime occurs when, outside of the cases provided for in Article 314 of the Criminal Code, a public official or person in charge of a public service, having by virtue of his office or service the possession or otherwise availability of money or other movable property belonging to others, allocates it for a use other than that provided for by specific provisions of law or by acts having the force of law from which no margin of discretion remains, and, as a result, entirely procures for himself or others an unjust financial advantage or unjust damage to others.

- ***Embezzlement by profiting from another's error (art. 316 of the Criminal Code)***

This type of crime occurs when a public official or person in charge of a public service, in the performance of his duties or service, takes advantage of the error of others and unduly receives or retains, for himself or for a third party, money or other benefits.

The crime may lead to the administrative liability of the Entity when the act harms the financial interests of the European Union.

- ***Embezzlement of public funds (art. 316-bis of the Italian Criminal Code)***

This type of crime occurs when, after receiving funding, contributions, subsidies, subsidized loans, or other similar disbursements, however named, intended for the achievement of one or more purposes by the Italian State or the European Union, the sums obtained are not used for the purposes for which they were intended (the conduct, in fact, consists of having diverted, even partially, the sum obtained, without it being relevant that the planned activity has in any case been carried out).

Given that the moment of commission of the crime coincides with the execution phase, the crime itself can also be configured with reference to payments already received in the past and which are now not used for the intended purposes.

- ***Undue receipt of public funds (Article 316-ter of the Criminal Code)***

This type of crime occurs when, through the use or presentation of false declarations or documents, or through the omission of required information, one obtains, without being entitled to them, contributions, subsidies, financing, subsidized loans, or other similar benefits granted or disbursed by the State, other public bodies, or the European Community.

In this case, contrary to what was seen in relation to the previous point (art. 316-*until*), it is irrelevant how the funds are used, since the crime is committed when the funding is obtained.

Finally, it should be emphasized that this criminal hypothesis is residual with respect to the crime of fraud against the State, in the sense that it only occurs in cases where the conduct does not meet the criteria for fraud against the State.

- **Disrupted freedom of auctions (art. 353 c.p.)**

The crime, also known as "bid-rigging", includes conduct aimed at preventing the auction (when the perpetrator of the crime acts to undermine the conditions for its performance) and that of driving away bidders (so as to ensure that, by dissuading potential participants, the auction fails), as well as the simpler conduct of "disruption", meaning any attitude that, although unsuitable for preventing the auction or driving away bidders, is capable of restricting or limiting the freedom of participants to submit their respective bids.

Pursuant to the sanctions provision, the effect of impeding or disrupting the tender can be achieved by using violence or threats to intimidate the bidders and/or public officials responsible for managing the tender procedure, or – conversely – by attempting to obtain the cooperation of the same parties in exchange for the offer or promise of donations, or by seeking a collusive agreement that allows the prospect of third parties obtaining undue advantages following the awarding of the tender.

- **Disturbed freedom of the contractor selection process (art. 353)*until* c.p.)**

The criminal conduct involves engaging in a specific type of interference with the tender process, namely, interference that occurs when the tender notice or other equivalent document is being finalized. The investigation requires the necessary cooperation of the public official in charge of the tender. Unlike the interference with the freedom of auctions referred to in Article 353 of the Criminal Code (a situation for which even a private individual can be held liable), the crime in question can only be committed when the public official interferes with the proper definition of the tender notice. This does not mean, however, that the public official must necessarily participate in the crime, since it is quite possible that the official's cooperation is due to the violence or threats he or she has suffered from the perpetrators of the crime.

- ***Fraud in public supplies (art. 356 of the Criminal Code)***

The crime occurs when fraud is committed in the execution of supply contracts or in the fulfillment of contractual obligations arising from a supply contract concluded with the State, or with another public entity, or with a company providing public services or public necessity services.

- ***Fraud against the European Agricultural Fund (Art. 2. Law 23 December 1986, n. 898)***

This type of crime occurs when, through the disclosure of false data or information, aid, prizes, compensation, refunds, contributions, or other benefits, fully or partially funded by the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development, are unduly obtained, for oneself or others.

- ***Concussion (art. 317 c.p.)***

This type of crime occurs when a public official or a person in charge of a public service, abusing their position or powers, forces someone to improperly give or promise money or other benefits to them or a third party. This crime is susceptible to merely residual application within the scope of the offenses covered by Legislative Decree 231/01; in particular, this type of crime could be identified, within the scope of Legislative Decree 231/01 itself, in the event that a Company employee or agent participates in the crime of a public official or a person in charge of a public service who, taking advantage of their position, requests undue services from third parties (provided that such behavior somehow benefits the Company).

The following persons are also included by "public official" and "public service officer":

1) the members of the Commission of the European Communities, of the European Parliament, of the Court of Justice and of the Court of Auditors of the European Communities;
2) officials and other agents employed under contract in accordance with the Staff Regulations of Officials of the European Communities or the Conditions of Employment of Agents of the European Communities;
3) persons seconded by Member States or by any public or private body 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, carry out functions and activities corresponding to those of public officials and persons in charge of a public service;
6) the judges, the Prosecutor, the Deputy Prosecutors, the officials and agents of the International Criminal Court, the persons seconded by the States Parties to the Treaty Establishing the International Criminal Court who exercise functions corresponding to those of officials or agents of the Court itself, the members and attachés of bodies established on the basis of the Treaty Establishing the International Criminal Court;

7) persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service within international public organisations;

8) members of international parliamentary assemblies or of an international or supranational organization and judges and officials of international courts;

9) persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service within non-EU countries, when the act harms the financial interests of the Union.

- ***Undue inducement to give or promise benefits (Article 319-quater of the Criminal Code)***

This criminal hypothesis, also called "***extortion by induction",*** It occurs when a public official or person in charge of a public service, abusing their position, induces someone to improperly give or promise money or other benefits to themselves or to a third party.

The penalty is six to ten years and six months' imprisonment for public officials and those in charge of a public service, and up to three years' imprisonment for anyone who gives or promises money or other benefits. The penalty is up to four years' imprisonment when the act harms the financial interests of the European Union and the damage or profit exceeds €100,000.

Punishability also extends to any private individual who is induced to pay or promise money or other benefits due to the abuse of power by a public official or public service employee. For the offense to be considered, the following elements must be present:

- a conduct of the active subject which must translate into an induction activity;
- an event embodied by two conducts of the passive subject (promise or undue giving of money or other benefit);
- an etiological link between induction and final event;
- the representation and volition of one's own unlawful action.

- ***Corruption in the exercise of one's function or to perform an act contrary to one's official duties (Articles 318, 319, 319-bis, 320 of the Criminal Code)***

These criminal offences arise when a public official receives, for himself or for others, money or other benefits to perform, omit or delay acts of his office (thus resulting in an advantage in favour of the offerer).
The activity of the public official may be expressed either in an obligatory act (for example: speeding up a procedure whose processing is his responsibility) or in an act contrary to his duties (for example: a public official who accepts money to guarantee the awarding of a tender).
In the event of an act contrary to one's duties, the penalty is increased if the act concerns the awarding of public positions or salaries or pensions or the stipulation of contracts in which the administration to which the public official belongs is involved.

The penalties provided for corruption for a duty also apply when the perpetrator is a public official, if he or she holds the status of a public employee.

The penalties provided for acts contrary to one's duties also apply if they are committed by a public official.

These crimes differ from extortion in that there is an agreement between the corrupt and the corrupter aimed at achieving a mutual advantage, while in extortion the private individual suffers the conduct of the public official or the person in charge of a public service.

Penalties are also provided for the briber (art. 321 of the Criminal Code).

The following persons are also included by "public official" and "public service officer":

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

2) officials and other servants engaged under contract in accordance with the Staff Regulations of Officials of the European Communities or the Conditions of Employment of Servants of the European Communities;

3) persons seconded by Member States or by any public or private body 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 and activities corresponding to those of public officials and persons in charge of a public service;

6) the judges, the Prosecutor, the Deputy Prosecutors, the officials and agents of the International Criminal Court, the persons seconded by the States Parties to the Treaty Establishing the International Criminal Court who exercise functions corresponding to those of officials or agents of the Court itself, the members and attachés of bodies established on the basis of the Treaty Establishing the International Criminal Court;

7) persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service within international public organisations;

8) members of international parliamentary assemblies or of an international or supranational organization and judges and officials of international courts;

9) persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service within non-EU countries, when the act harms the financial interests of the Union.

For the purposes of determining the penalties for the corrupt person, "public official" and "public service representative" are considered, in addition to the persons indicated in the

previous points, also persons who perform functions or activities corresponding to those of public officials and public service representatives within other foreign states or international public organizations, if the act is committed to obtain an undue advantage for themselves or others in international economic transactions.

- ***Corruption in judicial documents (Article 319-ter of the Criminal Code)***

This type of crime occurs when the Company is a party to a judicial proceeding and, in order to gain an advantage in the proceeding itself, bribes a public official (not only a magistrate, but also a clerk or other official).

- ***Incitement to corruption (Article 322 of the Criminal Code)***

This crime occurs when, in the presence of behavior aimed at corruption, the public official refuses the offer illicitly made to him.

The following persons are also included by "public official" and "public service officer":

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

2) officials and other servants engaged under contract in accordance with the Staff Regulations of Officials of the European Communities or the Conditions of Employment of Servants of the European Communities;

3) persons seconded by Member States or by any public or private body 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 and activities corresponding to those of public officials and persons in charge of a public service;

6) the judges, the Prosecutor, the Deputy Prosecutors, the officials and agents of the International Criminal Court, the persons seconded by the States Parties to the Treaty Establishing the International Criminal Court who exercise functions corresponding to those of officials or agents of the Court itself, the members and attachés of bodies established on the basis of the Treaty Establishing the International Criminal Court;

7) persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service within international public organisations;

8) members of international parliamentary assemblies or of an international or supranational organization and judges and officials of international courts;

9) persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service in non-EU countries, when the act harms the financial interests of the Union

- ***Embezzlement, misappropriation of money or movable property, extortion, undue inducement to give or promise benefits, corruption and incitement to corruption of members of the International Criminal Court or of bodies of the European Communities or of international parliamentary assemblies or international organizations and of officials of the European Communities and foreign states (Article 322-bis of the Criminal Code)***

The provisions of the articles314, 316, and317 a 320and322, third and fourth paragraphs, also apply:

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

2) to officials and agents employed under contract pursuant to the statute of the officials of the European Communities or of the conditions applicable to officials of the European Communities;

3) to persons seconded by Member States or by any public or private body to the European Communities, who perform functions corresponding to those of officials or agents of the European Communities;

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

5) to those who, within other Member States of the European Union, carry out functions or activities corresponding to those of the public officials and those responsible for a public service.

5-bis) to the judges, the Prosecutor, the Deputy Prosecutors, the officials and agents of the International Criminal Court, to the persons seconded by the States Parties to the Treaty establishing the International Criminal Court who exercise functions corresponding to those of officials or agents of the Court itself, to the members and employees of bodies established on the basis of the Treaty establishing the International Criminal Court[(2)].

5-ter) to persons who exercise functions or activities corresponding to those of thepublic officialsand those in charge of apublic servicewithin international public organizations;

5-quater) to members of international parliamentary assemblies or of ainternational organizationor supranational and to the judges and officials of international courts[(3)];

5-quinquies) to persons who exercise functions or activities corresponding to those of public officials and persons in charge of a public service within non-EU countries, when the act harms the financial interests of the Union[(4)].

The provisions of the articles319 quater, second paragraph[(5)], 321and322, first and second paragraphs, also apply if money or other benefits are given, offered or promised[(6)]:

1) to the persons indicated in the first paragraph of this article;

2) to persons who exercise functions or activities corresponding to those of the public officials and those in charge of public service within other foreign states or international public organizations[(7)(8)].

The persons indicated in the first paragraph are assimilated to public officials, when they exercise corresponding functions, and to those in charge of a public service in other cases.

- ***Illicit influence peddling (Article 346-bis of the Criminal Code)***

Anyone who, outside of cases of complicity in the crimes referred to in Articles 318, 319, and 319-ter and in the corruption crimes referred to in Article 322-bis, intentionally using existing relationships with a public official or a person in charge of a public service or one of the other persons referred to in Article 322-bis, unduly causes money or other economic benefits to be given or promised, to himself or to others, to remunerate a public official or a person in charge of a public service or one of the other persons referred to in Article 322-bis, in relation to the exercise of his functions, or to carry out other unlawful mediation, shall be punished with imprisonment for a term of one year and six months to four years and six months.

For the purposes of the first paragraph, other unlawful mediation means mediation to induce a public official or a person in charge of a public service or one of the other subjects referred to in Article 322-until to commit an act contrary to official duties, constituting a crime from which an undue advantage may be derived. Following the reform introduced by Law no. 114/2024 (the so-called Nordio Law), the offense was reformulated to make only the exploitation of existing relationships with a public official or person in charge of a public service a criminal offence for the purposes of establishing the conduct. The new formulation of the offense also defines the unlawful purposes that, for the purposes of typicality, render the promise or giving of money or other benefits undue and, specifically, constitute criminally relevant conduct pursuant to the new Article 346.*until* Criminal Code: the promise or delivery of money or other financial benefit that the mediator accepts or receives: either to remunerate a public official or a person in charge of a public service in relation to the performance of their duties; or, to carry out any other type of "unlawful mediation." From a subjective perspective, the recently reformed provision provides that the mediator is sanctioned for conduct committed "intentionally," excluding the relevance of any conduct committed as a result of merely possible intent.

- ***Fraud against the State, another public body, or the European Union (Article 640, paragraph 2, no. 1, of the Criminal Code)***

This type of crime occurs when, in order to obtain an unfair profit, tricks or deceptions are put in place that mislead and cause damage to the State (or to another Public Entity or to the European Union).

This crime may occur, for example, when, in preparing documents or data for participation in tender procedures, untrue information is provided to the Public Administration (for example, supported by falsified documentation or by entering non-existent names into the system), in order to obtain the awarding of the tender itself.

- ***Aggravated fraud to obtain public funds (Article 640-bis of the Criminal Code)***

This type of crime occurs when the fraud is carried out to unduly obtain public funds.

This situation may arise when tricks or deceptions are used, for example by communicating false information or preparing false documentation, to obtain public funding.

- ***Computer fraud against the State or another public body (Article 640-ter of the Criminal Code)***

This crime occurs when an unfair profit is obtained by altering the functioning of a computer or telematic system or manipulating the data contained therein, causing harm to third parties.

The crime is aggravated if one of the circumstances set out in number 1) of the second paragraph of article 640 occurs, or if the act produces a transfer of money, monetary value or virtual currency or is committed with abuse of the status of system operator, or where is committed through theft or improper use of the digital identity to the detriment of one or more individuals.

Specifically, the crime in question may be committed if, once financing has been obtained, the IT system is hacked to enter a financing amount higher than the amount legitimately obtained.

1.1 The Public Administration

The aim of this paragraph is to indicate general criteria and provide an illustrative list of those individuals classified as "active subjects" in the crimes relevant for the purposes of Legislative Decree 231/01, or of those individuals whose qualification is necessary to integrate the criminal offences envisaged therein.

1.1.1 Public administration bodies

For the purposes of criminal law, any legal person that has public interests in mind and carries out legislative, jurisdictional, or administrative activities pursuant to public law provisions and authoritative acts is commonly considered a "public administration body."

Although there is no definition of public administration in the Criminal Code, according to the Ministerial Report on the Code itself and in relation to the crimes provided for therein, those entities that carry out "all the activities of the State and other public bodies" are considered to belong to the public administration.

In attempting to formulate a preliminary classification of legal entities belonging to this category, it is possible to recall, lastly, Article 1, paragraph 2, of Legislative Decree 165/01 regarding the organization of employment within public administrations, which defines all State administrations as public administrations.

The distinctive characteristics of Public Administration bodies are summarized below.

<u>Public Administration Body:</u>

Any entity that has public interests in mind, which carries out activities:

- **legislative- jurisdictional**
- **administrative by** virtue of:
- **public law provisions - of authoritative acts**

Public Administration:

All the state **activities and** other public bodies.

By way of example, the following entities or categories of entities may be indicated as Public Administration entities:

- Institutes and schools of all levels and educational institutions;
- State bodies and administrations with autonomous organisation, such as:
- Ministry;
- House and Senate;
- Department of Community Policies;
- Competition and Market Authority

- Electricity and Gas Authority;
- Communications Regulatory Authority;
- Bank of Italy;
- Consob;
- Italian Data Protection Authority;
- Revenue Agency;
- Regions;
- Province;
- Municipalities;
- Mountain communities, and their consortia and associations;
- Chambers of Commerce, Industry, Crafts and Agriculture, and their associations.

All national, regional and local non-economic public bodies, such as:

- INPS;
- CNR;
- INAIL;
- STATE;
- ENASARCO;
- ASL;
- State Bodies and Monopolies;
- RAI.

Without prejudice to the purely exemplary nature of the public bodies listed above, it should be noted that not all natural persons acting within the sphere and in relation to the aforementioned bodies are subjects against whom (or by whom) the criminal offences are committed.*ex* D.Lgs. 231/01.

In particular, the figures that are relevant for this purpose are only those of "Public Officials" and "Public Service Persons".

1.1.2 Public Officials

Pursuant to Article 357, first paragraph, of the Criminal Code, a public official is considered "*for the purposes of criminal law*"he who exercises"*a public legislative, judicial or administrative function*".

The second paragraph then defines the concept of "public administrative function." However, no similar definitional effort has been undertaken to clarify the concepts of "legislative function" and "judicial function," as identifying the entities that exercise them has generally not given rise to any particular problems or difficulties.

Therefore, the second paragraph of the article in question specifies that, for the purposes of the criminal law "*public is the administrative function governed by public law provisions and by authoritative acts and characterised by the formation and manifestation of the will of the public administration or by its performance by means of authoritative or certifying powers*".

In other words, an administrative function governed by "public law" rules is defined as public, that is, by those rules aimed at pursuing a public purpose and protecting a public interest and, as such, contrasted with private law rules.

The second paragraph of Article 357 of the Criminal Code translates into normative terms some of the main criteria identified by case law and legal doctrine to differentiate the concept of "public function" from that of "public service."

The distinctive features of the first figure can be summarized as follows:

Public Official: Someone who exercises a public legislative, judicial or administrative function.

Public administrative functionAdministrative function governed by public law and authoritative acts; characterized by:

- formation and manifestation of the will of the public administration, or - carried out by means of authoritative or certifying powers.
- Public law provisions: Rules aimed at pursuing a public purpose and protecting a public interest.
- Foreign Public Officials:
- any person exercising a legislative, administrative or judicial function in a foreign country;
- any person exercising a public function for a foreign country or for a public body or public enterprise of that country;
- any official or agent of a public international organization.

1.1.3 Persons entrusted with a public service

The definition of the category of "persons entrusted with a public service" is currently not consistent in legal doctrine or case law. To better define this category of "persons entrusted with a public service," it is necessary to refer to the definition provided by the Criminal Code and the interpretations that have emerged following practical application. In particular, Article 358 of the Criminal Code states that "*Those who, in any capacity, provide a public service are entrusted with a public service.*

By public service we mean an activity regulated in the same ways as public function, but characterised by the lack of the powers typical of the latter, and with exclusion of the performance of simple administrative tasks and the provision of merely material work".

In order for a "service" to be defined as public, it must be regulated – just like a "public function" – by public law provisions, however, without the certification, authorization, and deliberative powers inherent to a public function.

The law also specifies that the performance of “simple administrative tasks” or the “provision of merely material work” can never constitute a “public service”.

Case law has identified a series of "indicators" that indicate the public nature of an entity, particularly the case of publicly held joint-stock companies. Specifically, the following indicators are used:

- subjection to control and direction for social purposes, as well as to the power to appoint and dismiss directors by the State or other public bodies;
- the presence of an agreement and/or concession with the public administration;
- the financial contribution from the State;
- the presence of public interest within economic activity.

On the basis of the above, the discriminating element to indicate whether or not a subject holds the status of "person in charge of a public service" is represented not by the legal nature assumed or held by the entity, but by the entrusted functions to the subject which must consist of the care of public interests or in the satisfaction of needs of general interest.

The specific characteristics of the public service employee are summarised in the following table:

Public Service Representatives: Those who, in any capacity, provide a public service.

Public service: An activity:

- governed by public law provisions;
- characterized by the lack of deliberative, authoritative and certifying powers (typical of the public administrative function), and - The performance of simple administrative tasks or the provision of merely material work can never constitute a public service.

2. The types of crimes of "computer crime" (art. 24-*until*of D.Lgs. 231/01)

- Law no. 48/2008 ratifying the Convention on Cybercrime introduced art. 13 of Legislative Decree 231/01.**24-*until***, which has extended the responsibility administrative of people legal to**"Computer Crime" crimes**Article 24*until* It was significantly amended by Law no. 90/2024, the so-called Cybersecurity Law, which increased the sanctions applicable to entities for crimes of this nature committed in their interest or to their advantage. The reform also added to Article 24-*until*the new paragraph 1-*until*, according to which the pecuniary sanction of between three hundred and eight hundred quotas is applied to the entity following the commission of the new type of crime – also introduced by the Cybersecurity Law – linked to cyber extortion (*ex* art. 629 comma 3 c.p.).

Art. 24-bis

Computer crimes and unlawful data processing

1. *In relation to the commission of the crimes referred to in Articles 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater and 635-quinquies of the Criminal Code, the entity shall be subject to a pecuniary sanction ranging from two hundred to seven hundred shares.*

1-bis. In relation to the commission of the crime referred to in Article 629, third paragraph, of the Criminal Code, the entity shall be subject to a pecuniary sanction ranging from three hundred to eight hundred shares.

2. *In relation to the commission of the crimes referred to in Articles 615-quater and 635-quater.1 of the Criminal Code, the entity is subject to a pecuniary sanction of up to four hundred quotas.*
3. *In relation to the commission of the crimes referred to in Articles 491-bis and 640-quinquies of the Criminal Code, except as provided in Article 24 of this decree for cases of computer fraud to the detriment of the State or another public entity, ((and the crimes referred to in Article 1, paragraph 11, of Legislative Decree 21 September 2019, no. 105,)) the entity shall be subject to a pecuniary sanction of up to four hundred quotas.*
4. *In cases of conviction for one of the crimes indicated in paragraph 1, the interdictory sanctions provided for in Article 9, paragraph 2, letters a), b) and e) shall apply. In cases of conviction for one of the crimes indicated in paragraph* 1 *until* The interdictory sanctions provided for in Article 9, paragraph 2, shall apply for a period of no less than two years. In cases of conviction for one of the crimes indicated in paragraph*2. The interdictory sanctions provided for in Article 9, paragraph 2, letters b) and e) apply. In cases of conviction for one of the crimes indicated in paragraph 3, the interdictory sanctions provided for in Article 9, paragraph 2, letters c), d) and e) apply.*

The individual cases contemplated in Legislative Decree 231/01, art. 24, are briefly described below.*until:*

- **[Falsehoods regarding] computer documents** ***(art. 491bis c.p.)***

If any of the false statements provided for in this chapter concern a public electronic document having evidentiary value, the provisions of the same chapter concerning public documents shall apply.

- ***Unauthorized access to a computer or telematic system (Article 615-ter of the Criminal Code)***

Anyone who unlawfully enters a computer or telematic system protected by security measures, or remains there against the express or imprisoned will of anyone who has the right to exclude him, is punishable by imprisonment of up to three years.

The penalty is imprisonment from two to ten years:

1) if the act is committed by a public official or by a person in charge of a public service, with abuse of power, or with violation of the duties inherent to the function or service, or by someone who practices the profession of private investigator, even abusively, or with abuse of the position of system operator;
2) if the guilty party uses violence against property or people to commit the act, or if he is clearly armed;
3) if the act results in the destruction or damage of the system or the total or partial interruption of its functioning, or the destruction or damage or the theft, including through reproduction or transmission, or the inaccessibility to the owner of the data, information or programs contained therein.

If the acts referred to in the first and second paragraphs involve computer or telematic systems of military interest or relating to public order or public safety, or to health or civil defense, or otherwise of public interest, the penalty is imprisonment for three to ten years and four to twelve years, respectively. In the case referred to in the first paragraph, the crime is punishable upon complaint by the injured party; in other cases, prosecution is ex officio.

- ***Illegal possession, distribution, and installation of equipment, codes, and other means for accessing computer or telematic systems (Article 615-quater of the Criminal Code)***

Anyone who, for the purpose of obtaining a profit for himself or others or causing harm to others, unlawfully procures, possesses, produces, reproduces, disseminates, imports, communicates, delivers, otherwise makes available to others, or installs equipment, instruments, parts of equipment or other instruments, codes, passwords, or other means suitable for accessing a computer or telematic system protected by security measures, or in any case provides indications or instructions suitable for the aforementioned purpose, is punishable by imprisonment of up to two years and a fine of up to five thousand one hundred and sixty-four euros.

The penalty is imprisonment from two to six years when one of the circumstances referred to in art. 615 occurs.*to have,* second paragraph, number 1.

The penalty is imprisonment from three to eight years when the act involves information or telematic systems as per Article 615-ter, third paragraph.

- ***Unlawful interception, impediment, or interruption of computer or telematic communications (Article 617-quater of the Criminal Code)***

Anyone who fraudulently intercepts communications relating to a computer or telematic system or between multiple systems, or prevents or interrupts them, is punishable by imprisonment for one year and six months to five years. Unless the act constitutes a more serious crime, the same penalty applies to anyone who discloses, through any means of information to the public, in whole or in part, the content of the communications referred to in the first paragraph.

The crimes referred to in the first and second paragraphs are punishable upon complaint by the injured party.

However, the proceedings are carried out ex officio and the penalty is imprisonment from four to ten years if the act is committed:

1) to the detriment of any of the computer systems indicated in art. 615*to have*, third paragraph;
2) to the detriment of a public official in the exercise or because of his functions or by a public official or by a person in charge of a public service, with abuse of powers or with violation of duties inherent to the function or service, or with abuse of the position of system operator.

- ***Illegal possession, distribution, and installation of equipment and other means designed to intercept, prevent, or interrupt computer or telematic communications (Article 617-quinquies of the Criminal Code)***

Anyone who, outside of the cases permitted by law, for the purpose of intercepting communications relating to a computer or telematic system or between multiple systems, or to prevent or interrupt them, procures, possesses, produces, reproduces, disseminates, imports, communicates, delivers, otherwise makes available to others or installs equipment, programs, codes, keywords or other means capable of intercepting, preventing or interrupting communications relating to a computer or telematic system or between multiple systems, is punishable by imprisonment from one to five years in the cases provided for in the fourth paragraph of Article 617.*quarter*

When one of the circumstances referred to in Article 617 occurs quarter, fourth paragraph, number 2), the penalty is imprisonment from two to six years.

When one of the circumstances referred to in Article 617 occurs quarter, fourth paragraph, number 1), the penalty is imprisonment from three to eight years.

- ***Damage to information, data, and computer programs (Article 635-bis of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who destroys, damages, deletes, alters or suppresses information, data or computer programs belonging to others is punishable, upon complaint of the injured party, by imprisonment from two to six years.

The penalty is imprisonment from three to eight years:

1) if the act is committed by a public official or by a person in charge of a public service, with abuse of power or violation of duties inherent to the function or service, or by someone who practices, even abusively, the profession of private investigator, or with abuse of the quality of system operator;
2) if the perpetrator uses threats or violence to commit the crime or is clearly armed.

- ***Damage to information, data, and computer programs used by the State or another public body or entity of public utility (Article 635-ter of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who commits an act aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs of military interest or relating to public order or public safety or health or civil protection or in any case of public interest, is punishable by imprisonment for two to six years.

The penalty is imprisonment from three to eight years:

1) if the act is committed by a public official or by a person in charge of a public service, with abuse of power or violation of duties inherent to the function or service, or by someone who practices, even abusively, the profession of private investigator, or with abuse of the quality of system operator;
2) if the guilty party uses threats or violence to commit the act or if he is clearly armed;
3) if the act results in the destruction, deterioration, cancellation, alteration or suppression of information or the theft, including through reproduction or transmission, or the inaccessibility of the data or computer programs to the legitimate owner.

The penalty is imprisonment from four to twelve years when one of the circumstances referred to in numbers 1) and 2) of the second paragraph concurs with one of the circumstances referred to in number 3).

- ***Damage to computer or telematic systems (Article 635-quater of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who, through the conduct referred to in Article 635*until*, or through the introduction or transmission of data, information or programs, destroys, damages, renders, in whole or in part, unusable the computer or telematic systems of others or seriously hinders their functioning is punishable by imprisonment from two to six years.

The penalty is imprisonment from three to eight years:

1. if the act is committed by a public official or by a person in charge of a public service, with abuse of power or violation of duties inherent to the function or service, or by someone who practices, even abusively, the profession of private investigator, or with abuse of the quality of system operator;
2. if the guilty party uses threats or violence to commit the act or if he is clearly armed.

- ***Illegal possession, distribution, and installation of computer equipment, devices, or programs intended to damage or disrupt a computer or telematics system (Article 635-quater.1 of the Criminal Code)***

Anyone who, with the aim of unlawfully damaging a computer or telematic system or the information, data, or programs contained therein or pertaining to it, or of facilitating the total or partial interruption or alteration of its functioning, unlawfully procures, holds, produces, reproduces, imports, disseminates, communicates, delivers, or in any case makes available to others or installs computer equipment, devices, or programs, is punishable by imprisonment of up to two years and a fine of up to €10,329.
The penalty is imprisonment from two to six years when one of the circumstances referred to in Article 615 occurs.*to have*, second paragraph, number 1).
The penalty is imprisonment from three to eight years when the act concerns the computer or telematic systems referred to in art. 615*to have,* third paragraph.

- ***Damage to information technology or telematic systems of public interest (Article 635-quinquies of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who, through the conduct referred to in Article 635 bis or through the introduction or transmission of data, information or programs, carries out acts aimed at destroying, damaging or rendering, in whole or in part, unusable information technology or telematic systems of public interest or at seriously hindering their functioning shall be punished with imprisonment for a term of two to six years.
The penalty is imprisonment from three to eight years:

1) if the act is committed by a public official or by a person in charge of a public service, with abuse of power or violation of duties inherent to the function or service, or by someone who practices, even abusively, the profession of private investigator, or with abuse of the quality of system operator;
2) if the guilty party uses threats or violence to commit the act or if he is clearly armed;
3) if the act results in the destruction, deterioration, cancellation, alteration or suppression of information, data or computer programs.

The penalty is imprisonment from four to twelve years when one of the circumstances referred to in numbers 1) and 2) of the second paragraph concurs with one of the circumstances referred to in number 3).

- ***Computer fraud by a person providing electronic signature certification services (Article 640-quinquies of the Criminal Code)***

Any person providing electronic signature certification services who, for the purpose of obtaining an unfair profit for themselves or others or causing harm to others, violates the legal obligations for issuing a qualified certificate is punishable by imprisonment of up to 3 years and a fine of 51 to 1,032 euros.

- ***Obstruction or conditioning of the implementation of national cybersecurity measures (Article 1, paragraph 11, of Legislative Decree no. 105 of 21 September 2019)***

Anyone who, with the aim of hindering or influencing the performance of the proceedings referred to in paragraph 2, letter b), or paragraph 6, letter a), or the inspection and supervisory activities referred to in paragraph 6, letter c), provides untrue information, data, or factual elements relevant to the preparation or updating of the lists referred to in paragraph 2, letter b), or for the purposes of the communications referred to in paragraph 6, letter a), or for the performance of the inspection and supervisory activities referred to in paragraph 6, letter c), or fails to communicate the aforementioned data, information, or factual elements within the prescribed time limits, shall be punished with imprisonment for one to three years.

So-called computer-based extortion (Article 629, paragraph 3, of the Criminal Code)

Anyone who, through the conduct referred to in Articles 615-*to have*, 617-*quarter*, 617-*sexies*, 635-*until*, 635-*quarter*and 635-*five times*or, by threatening to do so, forces someone to do or omit something, thereby obtaining an unjust profit for himself or others at the expense of others, is punishable by six to twelve years' imprisonment and a fine of €5,000 to €10,000. The penalty is eight to twenty-two years' imprisonment and a fine of €6,000 to €18,000 if any of the circumstances indicated in the third paragraph of Article 628 are present, as well as if the act is committed against a person incapacitated due to age or infirmity.

3. The types of organized crime offenses (Article 24-ter of Legislative Decree 231/01)

Law no. 94 of 15 July 2009, art. 2, paragraph 29, introduced organized crime offences within the scope of art. 24-ter of Legislative Decree 231/01.

Art. 24-ter

Organized crime crimes

1. *In relation to the commission of any of the crimes referred to in Articles 416, sixth paragraph, 416-bis, 416-ter, and 630 of the Criminal Code, to crimes committed by taking advantage of the conditions set forth in the aforementioned Article 416-bis or in order to facilitate the activities of the associations referred to in the same Article, as well as to the crimes referred to in Article 74 of the consolidated text referred to in Presidential Decree No. 309 of 9 October 1990, a pecuniary sanction of between four hundred and one thousand quotas shall apply.*
2. *In relation to the commission of any of the crimes referred to in Article 416 of the Criminal Code, with the exception of the sixth paragraph, or referred to in Article 407, paragraph 2, letter a), number 5), of the Code of Criminal Procedure, a pecuniary sanction of between three hundred and eight hundred quotas shall apply.*
3. *In cases of conviction for one of the crimes indicated in paragraphs 1 and 2, the disqualification sanctions provided for in Article 9, paragraph 2, shall apply for a period of no less than one year.*
4. *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 crimes indicated in*

paragraphs 1 and 2, the sanction of permanent disqualification from exercising the activity pursuant to Article 16, paragraph 3, shall apply.

The individual cases covered by Article 24-ter of Legislative Decree 231/01 are briefly described below.

- Criminal association (art. 416, paragraph 6, c.p.)

1. When three or more people join together for the purpose of committing multiple crimes, those who promote, constitute, or organize the association shall be punished, for that alone, with imprisonment from three to seven years.

2. For the mere fact of participating in the association, the penalty is imprisonment from one to five years.

3. The leaders are subject to the same penalty established for the promoters.

4. If the associates roam the countryside or public streets armed, the penalty is imprisonment from five to fifteen years.

5. The penalty is increased if the number of members is ten or more.

6. If the association is aimed at committing one of the crimes referred to in Articles 600, 601, 601-bis and 602, as well as Article 12, paragraph 3-*until*, of the consolidated text of the provisions concerning the regulation of immigration and rules on the status of foreigners, pursuant to Legislative Decree 25 July 1998, n. 286 as well as Articles 22, paragraphs 3 and 4, 22-bis, paragraph 1 of Law 1 April 1999, n. 91, imprisonment from five to fifteen years applies in the cases provided for in the first paragraph and from four to nine years in the cases provided for in the second paragraph.[2].

7. If the association is aimed at committing one of the crimes provided for in Articles 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 609-bis, when the act is committed

[2]The criminal offences provided for in Articles 600, 601, 601-bis, and 602 of the Criminal Code are described in the section on Crimes against the Individual, provided for in Article 25-quinquies of Legislative Decree 231/01.
Article 12, paragraphs 3 and 3-*until* , of Legislative Decree 25 July 1998, n. 286 (Provisions against illegal immigration) provides: “Unless the act constitutes a more serious crime, anyone who, in violation of the provisions of this consolidated law, promotes, directs, organizes, finances or carries out the transport of foreigners into the territory of the State or carries out other acts aimed at illegally procuring their entry into the territory of the State, or of another State of which the person is not a citizen or does not have a permanent residence permit, shall be punished with imprisonment from five to fifteen years and with a fine of €15,000.00 for each person in the event that: a) the act concerns the illegal entry or stay in the territory of the State of five or more persons; b) the transported person has been exposed to danger to his life or safety in order to procure his illegal entry or stay; c) the transported person has been subjected to inhuman or degrading treatment in order to procure his illegal entry or stay; d) the act is committed by three or more persons in complicity with each other or using international transport services or counterfeit or altered documents or otherwise illegally obtained; e) the perpetrators of the crime have access to weapons or explosives. 3-*until*If the acts referred to in paragraph 3 are committed when two or more of the hypotheses referred to in letters a), b), c), d) and e) of the same paragraph apply, the penalty provided therein is increased. (*omitted*)

against a minor under eighteen years of age, 609-quater, 609-quinquies, 609-octies, when the act is committed against a minor under eighteen years of age, and 609-undecies, imprisonment from four to eight years shall apply in the cases provided for in the first paragraph and imprisonment from two to six years in the cases provided for in the second paragraph.

- Mafia-type associations, including foreign ones (Article 416-bis of the Criminal Code)

Anyone who is part of a mafia-type organization consisting of three or more people is punishable by ten to fifteen years of imprisonment. Those who promote, direct, or organize the organization are punishable, for that alone, by twelve to eighteen years of imprisonment.
An association is mafia-type when its members exploit the intimidating power of membership and the resulting condition of subjugation and silence to commit crimes, to directly or indirectly acquire management or control of economic activities, concessions, authorizations, contracts, and public services, or to obtain unfair profits or advantages for themselves or others.

If the association is armed, the penalty is from twelve to twenty years of imprisonment in the cases provided for in the first paragraph and from fifteen to twenty-six years in the cases provided for in the second paragraph.

The association is considered armed when the participants have access to weapons or explosives, even if hidden or kept in a storage area, to achieve the association's purpose.

If the economic activities over which the associates intend to assume or maintain control are financed in whole or in part with the price, product, or profit of crimes, the penalties established in the previous paragraphs are increased by one-third to one-half. The convicted person is always subject to mandatory confiscation of the items used or intended to commit the crime and of the items that constitute its price, product, profit, or use.

The provisions of this article also apply to the Camorra, the ‘Ndrangheta, and other associations, however locally named, including foreign ones, which, by making use of the intimidating power of the associative bond, pursue aims corresponding to those of mafia-type associations.

- ***Political-mafia electoral exchange (Article 416-ter of the Criminal Code)***

Anyone who accepts, directly or through intermediaries, the promise to procure votes from individuals belonging to the associations referred to in Article 416-bis or through the methods referred to in the third paragraph of Article 416-bis in exchange for the provision or promise of provision of money or any other benefit or in exchange for the willingness to satisfy the interests or needs of the mafia association shall be punished with the penalty established in the first paragraph of Article 416-bis.

The same penalty applies to anyone who promises, directly or through intermediaries, to procure votes in the cases referred to in the first paragraph.

If the person who accepted the promise of votes, following the agreement referred to in the first paragraph, is elected in the relevant electoral consultation, the penalty provided for in the first paragraph of Article 416-bis shall apply, increased by half.

In the event of conviction for the crimes referred to in this article, perpetual disqualification from holding public office always ensues.

- ***Kidnapping for the purpose of extortion (Article 630 of the Criminal Code)***

Whoever kidnaps a person for the purpose of obtaining, for himself or others, an unjust profit as the price of release, shall be punished with imprisonment from twenty-five to thirty years.

If the kidnapping results in the death of the kidnapped person, as a consequence not intended by the offender, the guilty party is punished with thirty years of imprisonment.

If the guilty party causes the death of the kidnapped person, the penalty is life imprisonment.

The penalties set forth in Article 605 shall apply to the participant who, by dissociating himself from the others, works to ensure that the taxable person regains his freedom, without this result being a consequence of the price of release.

However, if the taxpayer dies as a result of the kidnapping, after being released, the penalty is imprisonment from six to fifteen years.

For any participant who, dissociating himself from the others, works, outside the case provided for in the previous paragraph, to prevent the criminal activity from leading to further consequences or concretely assists the police or judicial authorities in gathering decisive evidence for the identification or capture of the participants, the penalty of life imprisonment is replaced by that of imprisonment from twelve to twenty years and the other penalties are reduced by one-third to two-thirds.

When a mitigating circumstance occurs, the penalty provided for in the second paragraph is replaced by imprisonment from twenty to twenty-four years; the penalty provided for in the third paragraph is replaced by imprisonment from twenty-four to thirty years.

If several mitigating circumstances occur, the penalty to be applied as a result of the reductions cannot be less than ten years, in the case provided for in the second paragraph, and fifteen years, in the case provided for in the third paragraph.

The penalty limits set out in the previous paragraph may be exceeded when the mitigating circumstances referred to in the fifth paragraph of this article apply.

- ***Criminal conspiracy for the purpose of trafficking narcotic or psychotropic substances (Article 74 of Presidential Decree 309/1990 - Consolidated Law on Narcotics)***

When three or more people join together for the purpose of committing multiple crimes among those set forth in Article 73, anyone who promotes, establishes, directs, organizes, or finances the association is punishable for that alone by a prison term of no less than twenty years. Anyone who participates in the association is punished by a prison term of no less than ten years. The penalty is increased if the number of members is ten or more

or if the participants include individuals addicted to the use of narcotic or psychotropic substances. If the association is armed, the penalty, in the cases indicated in paragraphs 1 and 3, cannot be less than twenty-four years of imprisonment and, in the case provided for in paragraph 2, twelve years of imprisonment. The association is considered armed when its participants have access to weapons or explosives, even if concealed or stored in a warehouse. The penalty is increased if the circumstance referred to in letter e) of paragraph 1 of Article 80 occurs. If the association is formed to commit the acts described in paragraph 5 of Article 73, the first and second paragraphs of Article 416 of the Criminal Code apply.

The penalties provided for in paragraphs 1 to 6 are reduced by half to two-thirds for those who have effectively worked to secure evidence of the crime or to remove from the association resources crucial to the commission of the crimes.

- ***Art. 407, paragraph 2, letter a), no. 5 of the Code of Criminal Procedure. Crimes of illegal manufacturing, introduction into the State, offering for sale, transfer, possession and carrying in a public place or open to the public of war or war-type weapons or parts thereof, explosives, clandestine weapons as well as multiple common firearms excluding those provided for in art. 2, paragraph 3 of Law 110/7***

4. The types of transnational crimes (Law no. 146 of 16 March 2006)

Law no. 146 of 16 March 2006, published in the Official Journal on 11 April 2006, ratified and implemented the United Nations Convention and Protocols against Transnational Organized Crime, adopted by the General Assembly on 15 November 2000 and 31 May 2001 (the so-called Palermo Convention).

The core of the Convention is the notion of *transnational crime*(art. 3). This is the crime which (i) goes beyond, in one or more aspects (preparatory, commission or effectual), the borders of a single State, (ii) is committed by a criminal organisation and

(iii) it is characterised by a certain gravity (it must be punished in the individual legal systems with a maximum prison sentence of no less than four years).

What is relevant, therefore, is not the occasional transnational crime, but the crime resulting from an organizational activity with stability and strategic perspective, and therefore susceptible to being repeated over time.

The law ratifying the Palermo Convention broadens the scope of Legislative Decree 231/01: pursuant to Article 10 of the law itself, the provisions of Legislative Decree 231/01 apply to the transnational crimes indicated in Law 146/2006.

The law defines transnational crime as a crime, punishable by a maximum term of imprisonment of not less than four years, involving an organized criminal group and which:

- is committed in more than one State; or
- is committed in one State, but a substantial part of its preparation, planning, direction or control takes place in another State; or

- is committed in one State, but involves an organised criminal group engaged in criminal activities in more than one State; or
- is committed in one State but has substantial effects in another State.

The Company is liable for the following crimes, committed in its interest or to its advantage, if they have a transnational character as defined above.

Crimes of association

- ***Criminal association (art. 416 of the Criminal Code)***
- ***Mafia-type association (Article 416-bis of the Criminal Code)***
- ***Association for the purpose of illicit trafficking of narcotic or psychotropic substances (Article 74 of Presidential Decree No. 309/1990)***[3]

- ***Criminal conspiracy aimed at smuggling manufactured tobacco (Article 86 of Legislative Decree 141/2024)***

This crime occurs when three or more people conspire to introduce, sell, transport, purchase, or possess within the Italian territory a quantity of contraband foreign-produced tobacco exceeding fifteen kilograms. Those who promote, establish, direct, organize, or finance such activities are punishable by three to eight years in prison. Those who participate are punished by one to six years in prison.

Migrant smuggling crimes

- ***Migrant trafficking (Article 12, paragraphs 3, 3-bis, 3-ter, and 5 of Legislative Decree no. 286/1998)***

This crime occurs when a person commits acts aimed at procuring the entry of another person into the country in violation of immigration laws, or acts aimed at procuring illegal entry into another country of which the person is not a citizen or does not have permanent residency, or, with the aim of unfairly profiting from the foreigner's illegal status, facilitating their permanence. In such cases, the punishment is four to fifteen years of imprisonment and a fine of €15,000 for each person (depending on the individual criminal offense, the penalties may be increased as provided for in the aforementioned provisions).

In this case, the company is subject to a fine ranging from two hundred to one thousand shares and a disqualification sanction of up to two years. The fine can therefore reach approximately €1.5 million (in particularly serious cases, the fine can be tripled).

In the event of the commission of migrant trafficking crimes, the entity is subject to disqualification sanctions for a period not exceeding two years.

[3]The criminal offences provided for by articles 416, 416*until* and art. 74 of Presidential Decree no. 309/1990. are described in the paragraph relating to*Organized crime crimes*provided for in art. 24*to have* of D.Lgs. 231/01.

Obstruction of justice offenses

- ***Inducement to withhold or make false statements to the judicial authority (Article 377-bis of the Criminal Code)***

This crime occurs when a person, through violence or threats, or by offering or promising money or other benefits, induces a person called to testify before a judicial authority that may be used in criminal proceedings, when the person has the right to remain silent, not to testify or to make false statements. In this case, the punishment is two to six years of imprisonment.

- ***Personal aiding and abetting (art. 378 of the Criminal Code)***

This crime occurs when someone assists a person in evading investigations or evading searches by the authorities following the commission of a crime. This offense carries a prison sentence of up to four years.

In the aforementioned cases, the company is subject to a fine of up to five hundred shares. The fine can therefore reach approximately €775,000. There are no disqualification sanctions for these types of crimes.

5. Crimes relating to "counterfeiting of coins, public credit cards, revenue stamps and distinctive instruments or signs" and crimes against industry and commerce (articles 25-*until*and 25-*until*1 of D.Lgs. 231/01)

Art. 25-bis
Counterfeiting of coins, public credit cards, stamps and instruments or signs of recognition

1. *In relation to the commission of crimes provided for by the Criminal Code regarding counterfeiting of coins, public credit cards, revenue stamps, and identifying instruments or signs, the following pecuniary sanctions apply to the entity:*
   - *a) for the crime referred to in Article 453, the pecuniary sanction ranges from three hundred to eight hundred shares;*
   - *b) for the crimes referred to in Articles 454, 460 and 461, a pecuniary sanction of up to five hundred quotas;*
   - *c) for the crime referred to in Article 455, the pecuniary sanctions established by letter a), in relation to Article 453, and by letter b), in relation to Article 454, reduced by one third to one half;*
   - *d) for the crimes referred to in Articles 457 and 464, second paragraph, pecuniary sanctions of up to two hundred quotas;*
   - *e) for the crime referred to in Article 459, the pecuniary sanctions provided for in letters a), c) and d) are reduced by one third;*
   - *f) for the crime referred to in Article 464, first paragraph, a pecuniary sanction of up to three hundred quotas.*

   f-bis) for the crimes referred to in Articles 473 and 474, a pecuniary sanction of up to five hundred quotas.

2. *In cases of conviction for one of the crimes referred to in Articles 453, 454, 455, 459, 460, 461, 473 and 474 of the Criminal Code, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity for a period not exceeding one year.*

Art. 25-bis.1
Crimes against industry and commerce

1. *In relation to the commission of crimes against industry and commerce provided for by the Criminal Code, the following pecuniary sanctions apply to the entity:*
   a) *for the crimes referred to in Articles 513, 515, 516, 517, 517-ter and 517-quater, a pecuniary sanction of up to five hundred quotas;*
   b) *for the crimes referred to in Articles 513-bis and 514, the pecuniary sanction is up to eight hundred quotas.*
2. *In the event of conviction for the crimes referred to in letter b) of paragraph 1, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity.*

The cases covered by Article 25 are briefly described below.*until* of the D.Lgs. 231/01 and, in particular, the crimes **relating to the counterfeiting of distinctive signs**(Articles 473 and 474 of the Criminal Code) introduced by Law 23 July 2009, n. 99, art.15, paragraph 7:

a. ***Counterfeiting of coins, spending and introduction into the State, by prior agreement, of counterfeit coins (Article 453 of the Criminal Code)***

The following are punishable by imprisonment from three to twelve years and a fine from €516.00 to €3,098.00:

1) anyone who counterfeits national or foreign coins, legal tender in the State or abroad;

2) anyone who alters genuine coins in any way, giving them the appearance of a higher value;

3) anyone who, without having participated in the counterfeiting or alteration, but in concert with the person who carried it out or with an intermediary, introduces into the territory of the State or holds or spends or otherwise puts into circulation counterfeit or altered coins;

4) anyone who, for the purpose of putting them into circulation, purchases or in any case receives counterfeit or altered coins from someone who counterfeited them, or from an intermediary.

The same penalty applies to anyone who, legally authorized to produce, unduly produces, by abusing the tools or materials at his disposal, quantities of coins in excess of the prescribed limits.

The penalty is reduced by a third when the conduct referred to in the first and second paragraphs involves coins that are not yet legal tender and the initial term of the penalty is determined.

b. ***Altering coins (art. 454 of the Criminal Code)***

Whoever alters coins of the quality indicated in the previous article, diminishing their value in any way, or, with respect to the coins thus altered, commits any of the acts indicated in numbers 3 and 4 of the said article, shall be punished with imprisonment from one to five years and with a fine from €103.00 to €516.00.

c. ***Spending and introducing counterfeit money into the State without agreement (Article 455 of the Criminal Code)***

Whoever, outside the cases provided for in the two preceding articles, introduces into the territory of the State, purchases or holds counterfeit or altered coins, with the aim of putting them into circulation, or spends them or otherwise puts them into circulation, is subject to the penalties established in the said articles reduced by between one third and one half.

d. ***Spending counterfeit money received in good faith (Article 457 of the Criminal Code)***

Anyone who spends or otherwise puts into circulation counterfeit or altered coins, received in good faith, is punishable by imprisonment of up to six months or a fine of up to €1,032.00.

e. ***Counterfeiting of revenue stamps, introduction into the country, purchase, possession, or circulation of counterfeit revenue stamps (Article 459 of the Criminal Code)***

The provisions of Articles 453, 455, and 457 also apply to the counterfeiting or alteration of revenue stamps and the introduction into Italian territory, or the purchase, possession, and circulation of counterfeit revenue stamps; however, the penalties are reduced by one-third. For the purposes of criminal law, revenue stamps are defined as stamped paper, revenue stamps, postage stamps, and other securities deemed equivalent to them by special laws.

f. ***Counterfeiting of watermarked paper used for the production of public credit cards or revenue stamps (Article 460 of the Criminal Code)***

Anyone who counterfeits watermarked paper used to manufacture public credit cards or revenue stamps, or purchases, holds, or sells such counterfeit paper, shall be punished, unless the act constitutes a more serious crime, with imprisonment from two to six years and a fine from €309.00 to €1,032.00.

g. ***Manufacture or possession of watermarks or instruments intended for the counterfeiting of coins, stamps or watermarked paper (art. 461 c.p.)***

Anyone who manufactures, purchases, possesses, or sells watermarks, computer programs and data, or tools intended for the counterfeiting or alteration of coins, revenue stamps, or watermarked paper shall be punished, unless the act constitutes a more serious crime, by imprisonment for one to five years and a fine of €103.00 to €516.00. The same penalty applies if the conduct referred to in the first paragraph involves holograms or other components of the currency intended to ensure its protection against counterfeiting or alteration.

h. ***Use of counterfeit or altered revenue stamps (Article 464 of the Criminal Code)***

Anyone who, without being involved in the counterfeiting or alteration, uses counterfeit or altered revenue stamps is punishable by imprisonment of up to three years and a fine of up to €516.

i. ***Counterfeiting, alteration or use of trademarks or distinctive signs or patents, models and designs (Article 473 of the Criminal Code)***

Anyone who, being aware of the existence of an industrial property title, counterfeits or alters national or foreign trademarks or distinctive signs of industrial products, or anyone who, without participating in the counterfeiting or alteration, uses such counterfeit or altered trademarks or signs, is punishable by imprisonment from six months to three years and a fine of between €2,500 and €25,000.

Anyone who counterfeits or alters national or foreign patents, designs, or industrial models, or, without participating in the counterfeiting or alteration, makes use of such counterfeit or altered patents, designs, or models, is subject to a prison sentence of one to four years and a fine of €3,500 to €35,000.

The crimes set forth in the first and second paragraphs are punishable provided that the provisions of internal laws, Community regulations and international conventions on the protection of intellectual or industrial property have been observed.

- Introduction into the State and trade of products with false markings (art. 474)

Except in cases of complicity in the crimes set forth in Article 473, anyone who introduces into the territory of the State, for the purpose of profit, industrial products bearing counterfeit or altered national or foreign trademarks or other distinctive signs is punishable by imprisonment for one to four years and a fine of between €3,500 and €35,000.

Except in cases of complicity in counterfeiting, alteration, or introduction into the territory of the State, anyone who holds for sale, offers for sale, or otherwise puts into circulation, for the purpose of profit, the products referred to in the first paragraph is punishable by imprisonment of up to two years and a fine of up to €20,000.

The crimes set forth in the first and second paragraphs are punishable provided that the provisions of internal laws, Community regulations and international conventions on the protection of intellectual or industrial property have been observed.

Law 23 July 2009, n. 99, art.15, paragraph 7 also introduced the**'art. 25-** ***until*** **l of Legislative Decree 231/01**, titled "**Crimes against industry and commerce",**the individual cases of which are described below:

- ***Disturbance of freedom of industry or commerce (art. 513 of the Criminal Code)***

Anyone who uses violence against property or fraudulent means to prevent or disrupt the operation of an industry or trade is punishable, upon complaint by the injured party, unless the act constitutes a more serious crime, by imprisonment for up to two years and a fine of between €103 and €1,032.

- ***Illicit competition with threats or violence (art. 513-bis c.p.)***

Anyone who, in the exercise of a commercial, industrial, or other productive activity, commits acts of competition with violence or threats is punishable by imprisonment for two to six years.

The penalty is increased if the acts of competition concern a financial activity in whole or in part and in any way by the State or other public bodies.

- ***Fraud against national industries (Article 514 of the Criminal Code)***

Anyone who, by selling or otherwise circulating, on domestic or foreign markets, industrial products with counterfeit or altered names, trademarks, or distinctive signs, causes harm to national industry is punishable by imprisonment for one to five years and a fine of not less than €516.

If the provisions of internal laws or international conventions on the protection of industrial property have been observed for the trademarks or distinctive signs, the penalty is increased and the provisions of Articles 473 and 474 do not apply.

- ***Fraud in the exercise of commerce (art. 515 of the Criminal Code)***

Anyone who, in the exercise of a commercial activity, or in a shop open to the public, delivers to the purchaser one movable good for another, or a movable good, in origin, provenance, quality, or quantity, different from that declared or agreed, is punishable, unless the act constitutes a more serious crime, by imprisonment of up to two years or a fine of up to €2,065.

If the objects involved are valuable, the penalty is imprisonment of up to three years or a fine of not less than 103 euros.

- ***Sale of non-genuine foodstuffs as genuine (Article 516 of the Criminal Code)***

Anyone who offers for sale or otherwise markets non-genuine food substances as genuine is punishable by imprisonment of up to six months or a fine of up to €1,032.00.

- ***Sale of industrial products with false markings (Article 517 of the Criminal Code)***

Anyone who holds for sale, offers for sale, or otherwise puts into circulation intellectual works or industrial products, with national or foreign names, trademarks, or distinctive signs, capable of misleading the buyer as to the origin, provenance, or quality of the work or product, shall be punished, unless the act is defined as a crime by another provision of law, with imprisonment of up to two years or a fine of up to twenty thousand euros.

- ***Manufacturing and trade of goods created by usurping industrial property rights (Article 517-ter)***

Without prejudice to the application of Articles 473 and 474, anyone who, being aware of the existence of an industrial property title, manufactures or uses industrially objects or other goods created by usurping an industrial property title or in violation of the same shall be punished, upon complaint of the injured party, with imprisonment of up to two years and a fine of up to 20,000 euros.

The same penalty applies to anyone who, for the purpose of profit, introduces into the territory of the State, holds for sale, offers for sale directly to consumers or otherwise puts into circulation the goods referred to in the first paragraph.

The provisions of Articles 474- shall apply.*until*, 474-*to have*, second paragraph, and 517-*until*, second paragraph.

The crimes set forth in the first and second paragraphs are punishable provided that the provisions of internal laws, community regulations and international conventions on the protection of intellectual or industrial property have been observed.

- ***Counterfeiting of geographical indications or designations of origin of agri-food products (Article 517-quater)***

Anyone who counterfeits or otherwise alters geographical indications or designations of origin of agri-food products is punishable by imprisonment of up to two years and a fine of up to €20,000.

The same penalty applies to anyone who, for the purpose of profit, introduces into the territory of the State, holds for sale, offers for sale directly to consumers, or otherwise puts into circulation the same products with counterfeit indications or names.

The provisions of Articles 474- shall apply.*until*, 474-*to have*, second paragraph, and 517-*until*, second paragraph.

The crimes set forth in the first and second paragraphs are punishable provided that the provisions of domestic laws, Community regulations, and international conventions regarding the protection of geographical indications and designations of origin for agri-food products have been observed.

6. The types of corporate crimes (art. 25-*ter* D.Lgs. 231/01)

Art. 25-ter

Corporate crimes

1. In relation to corporate crimes provided for by the civil code (or other special laws), the following pecuniary sanctions apply to the entity:
a) for the crime of false corporate communications provided for by Article 2621 of the Civil Code, a pecuniary sanction of between two hundred and four hundred shares;
a-bis) for the crime of false corporate communications provided for by Article 2621-bis of the Civil Code, a pecuniary sanction of between one hundred and two hundred shares;
b) for the crime of false corporate communications provided for by Article 2622 of the Civil Code, a pecuniary sanction of between four hundred and six hundred shares;
c) LETTER REPEALED BY LAW 27 MAY 2015, N. 69;
d) for the offence of false prospectus, as provided for by Article 2623, first paragraph, of the Civil Code, a pecuniary sanction of between one hundred and one hundred and thirty quotas;
e) for the crime of false prospectus, provided for by Article 2623, second paragraph, of the Civil Code, a pecuniary sanction of between two hundred and three hundred and thirty quotas;

f) for the violation of false information in the reports or communications of auditing firms, as provided for by Article 2624, first paragraph, of the Civil Code, a pecuniary sanction of between one hundred and one hundred and thirty quotas;
g) for the crime of false reporting in audit firms' reports or communications, as provided for in Article 2624, second paragraph, of the Civil Code, a pecuniary sanction of between two hundred and four hundred shares;
h) for the crime of obstruction of control, provided for by Article 2625, second paragraph, of the Civil Code, a pecuniary sanction of between one hundred and one hundred and eighty quotas;
i) for the crime of fictitious formation of capital, provided for by Article 2632 of the Civil Code, a pecuniary sanction of between one hundred and one hundred and eighty shares;
l) for the crime of undue restitution of contributions, provided for by Article 2626 of the Civil Code, a pecuniary sanction of between one hundred and one hundred and eighty shares;
m) for the contravention of illegal distribution of profits and reserves, provided for by Article 2627 of the Civil Code, a pecuniary sanction of between one hundred and one hundred and thirty shares;
n) for the crime of illicit transactions on shares or quotas of the company or of the controlling company, provided for by Article 2628 of the Civil Code, a pecuniary sanction of between one hundred and one hundred and eighty quotas;
o) for the crime of transactions to the detriment of creditors, provided for by Article 2629 of the Civil Code, a pecuniary sanction of between one hundred and fifty and three hundred and thirty shares;
p) for the crime of undue distribution of company assets by liquidators, provided for by Article 2633 of the Civil Code, a pecuniary sanction of between one hundred and fifty and three hundred and thirty shares;
q) for the crime of illicit influence on the assembly, provided for by article 2636 of the civil code, a pecuniary sanction of between one hundred and fifty and three hundred and thirty shares;
r) for the crime of stock market manipulation, provided for by Article 2637 of the Civil Code and for the crime of failure to communicate a conflict of interest provided for by Article 2629-bis of the Civil Code, a pecuniary sanction of between two hundred and five hundred shares;
s) for crimes of obstruction of the exercise of the functions of public supervisory authorities, provided for by Article 2638, first and second paragraphs, of the Civil Code, a pecuniary sanction of between two hundred and four hundred quotas;
s-bis) for the crime of corruption between private individuals, in the cases provided for in the third paragraph of Article 2635 of the Civil Code, a pecuniary sanction of between four hundred and six hundred shares and, in the cases of incitement referred to in the first paragraph of Article 2635-bis of the Civil Code, a pecuniary sanction of between two hundred and four hundred shares. The interdictory sanctions provided for in Article 9, paragraph 2, also apply.
((s-ter) for the crime of false or omitted declarations for the issuing of the preliminary certificate provided for by the implementing legislation of Directive (EU) 2019/2121, of the European Parliament and
of the Council, dated 27 November 2019, the pecuniary sanction of between one hundred and fifty and three hundred quotas.))
3. If, following the commission of the crimes referred to in paragraph 1, the entity has obtained a significant profit, the pecuniary sanction is increased by one third.

The individual cases contemplated in Legislative Decree 231/01, art. 25, are briefly described below.*to have:*

- ***False corporate communications (Article 2621 of the Civil Code)***

The crime occurs when directors, general managers, managers responsible for preparing corporate accounting documents, auditors, and liquidators, in order to obtain an unfair profit for themselves or others, knowingly disclose material facts that are untrue in financial statements, reports, or other corporate communications directed to shareholders or the public, as required by law, or omit material facts whose disclosure is required by law regarding the economic, financial, or asset situation of the company or the group to which it belongs, in a manner that is materially likely to mislead others.

In the event of the commission of this crime, the penalty is imprisonment for one to five years.

Liability also exists if the false statements or omissions concern assets owned or managed by the company on behalf of third parties.

- ***Minor incidents (art. 2621-bis)***

A lower penalty (from six months to three years of imprisonment) applies if the false corporate communications referred to in Article 2621 are of minor importance, also taking into account the nature and size of the company and the methods or effects of the conduct.

The same penalty also applies when the false corporate communications referred to in Article 2621 concern companies that do not exceed the limits indicated in the second paragraph of Article 1 of Royal Decree No. 267 of March 16, 1942 (i.e., companies not subject to bankruptcy). In this case, the crime is prosecutable upon complaint by the company, its shareholders, creditors, or other recipients of the corporate communication.

- ***False corporate communications by listed companies (Article 2622 of the Civil Code)***

The crime occurs when directors, general managers, managers responsible for preparing corporate accounting documents, auditors, and liquidators of companies issuing financial instruments admitted to trading on a regulated market in Italy or another European Union country, in order to obtain an unfair profit for themselves or others, knowingly present material facts in financial statements, reports, or other corporate communications addressed to shareholders or the public that are untrue or omit material facts that are required by law to be disclosed that are materially relevant to the economic, financial, or asset situation of the company or the group to which it belongs, in a manner that is concretely likely to mislead others.

In the event of the commission of this crime, the penalty is imprisonment from three to eight years.

The following are treated as companies issuing financial instruments admitted to trading on a regulated market in Italy or another European Union country:

1) companies issuing financial instruments for which an application for admission to trading on a regulated market in Italy or another European Union country has been submitted;
2) companies issuing financial instruments admitted to trading in an Italian multilateral trading facility;
3) companies that control companies issuing financial instruments admitted to trading on a regulated market in Italy or another European Union country;
4) companies that appeal to public savings or that in any case manage them.

The provisions of the preceding paragraphs also apply if the false statements or omissions concern assets owned or managed by the company on behalf of third parties.

- ***Prevented control (art. 2625 c.c.)[4]***

The crime consists in preventing or hindering, through the concealment of documents or other suitable artifices, the performance of control or auditing activities legally attributed to the shareholders, other corporate bodies, or auditing firms.

- ***Undue return of contributions (art. 2626 of the Civil Code)***

Typical conduct includes, outside of cases of legitimate reduction of share capital, the return, even simulated, of contributions to members or the release of the latter from the obligation to perform them.

- ***Illegal distribution of profits or reserves (Article 2627 of the Civil Code)***

This criminal conduct consists in distributing profits or advances on profits not actually earned or legally allocated to reserves, or distributing reserves, even if not constituted with profits, which cannot be distributed by law.

Please note that the return of profits or the reconstitution of reserves before the deadline for approval of the financial statements extinguishes the crime.

- ***Illegal transactions involving shares or quotas of a company or of the controlling company (Article 2628 of the Italian Civil Code)***

This crime is committed through the purchase or subscription of shares or quotas in a company or in the controlling company, which causes damage to the integrity of the share capital or reserves that are not legally distributable.

Please note that if the share capital or reserves are replenished before the deadline for approving the financial statements for the financial year in which the conduct occurred, the crime is extinguished.

- ***Transactions to the detriment of creditors (art. 2629 of the Civil Code)***

[4]Amended by art. 37, paragraph 35, of Legislative Decree no. 39 of 27 January 2010, which excludes auditing from the list of activities for which the law sanctions administrators' failure to perform.

This offence occurs when, in violation of the provisions of law protecting creditors, capital reductions or mergers with other companies or demergers are carried out, which cause damage to creditors.

It should be noted that compensation for damages to creditors before the trial extinguishes the crime.

- ***Failure to disclose a conflict of interest (Article 2629-bis of the Italian Civil Code)***

This offence occurs when the director or member of the management board of a company with securities listed on regulated markets in Italy or another European Union Member State or distributed to the public to a significant extent pursuant to Article 116 of the Consolidated Law pursuant to Legislative Decree No. 58 of 24 February 1998, as amended, or of a body subject to supervision pursuant to the Consolidated Law pursuant to Legislative Decree No. 385 of 1 September 1993, the aforementioned Consolidated Law pursuant to Legislative Decree No. 58 of 1998, Law No. 576 of 12 August 1982, or Legislative Decree No. 124 of 21 April 1993, fails to inform the other directors and the board of statutory auditors of any interest that he or she has, on his or her own behalf or on behalf of third parties, in a given transaction of the company, specifying its nature, terms, origin, and scope.

Please note that if the conflict of interest concerns the CEO, he must also refrain from carrying out the transaction, referring the matter to the collegiate body.

- ***Fictitious formation of capital (art. 2632 of the Civil Code)***

This situation occurs when: the company's capital is fictitiously created or increased by allocating shares or quotas for an amount lower than their nominal value; shares or quotas are reciprocally subscribed; contributions in kind, credits, or the company's assets, in the case of a transformation, are significantly overvalued.

- ***Improper distribution of company assets by liquidators (Article 2633 of the Civil Code)***

The crime is committed by distributing company assets among members before paying the company's creditors or setting aside the sums necessary to satisfy them, which causes damage to the creditors.

It should be noted that compensation for damages to creditors before the trial extinguishes the crime.

- ***Corruption between private individuals (art. 2635 c. 3 c.c.)***

The crime punishes anyone who, even through a third party, offers, promises, or gives undue money or other benefits to directors, general managers, managers responsible for preparing corporate accounting documents, auditors, liquidators, or anyone who, within the entity, exercises management functions other than those of the aforementioned individuals, or to individuals subject to their direction or supervision, in order for them to perform or omit acts in violation of the obligations inherent in their office or of the duties of loyalty, unless the conduct constitutes a more serious crime.

The penalty is imprisonment from one to three years and the crime is prosecutable ex officio,

- ***Incitement to corruption between private individuals (Article 2635-bis of the Civil Code)***

The crime punishes anyone who offers or promises money or other undue benefits to certain categories of people operating within companies or entities (directors, general managers, managers responsible for preparing corporate accounting documents, auditors, liquidators, as well as those who carry out work in private companies exercising managerial functions) to perform or omit an act in violation of the obligations inherent to their office or of the duties of loyalty, if the offer or promise is not accepted.

- ***Unlawful influence on the assembly (art. 2636 c.c.)***

Typical conduct involves determining, through simulated acts or fraud, a majority in an assembly with the aim of obtaining an unfair profit for oneself or others.

- ***Stock manipulation (art. 2637 of the Civil Code)***

This offence occurs when false information is spread or simulated transactions or other devices are implemented that are effectively capable of causing a significant change in the price of unlisted financial instruments or those for which no application for admission to trading on a regulated market has been submitted, or of significantly impacting the public's confidence in the financial stability of banks or banking groups.

- ***Obstruction of the exercise of the functions of public supervisory authorities (Article 2638, paragraphs 1 and 2 of the Civil Code)***

The criminal conduct is carried out through the disclosure, in communications to the supervisory authorities required by law, for the purpose of hindering their functions, of material facts that do not correspond to the truth, even if they are the subject of assessments, regarding the economic, patrimonial, or financial situation of the entities subject to supervision, or by concealing, through other fraudulent means, in whole or in part, facts that should have been communicated, concerning the same situation.

- ***False or omitted declarations for the issuance of the preliminary certificate*****(art. 54 of the Decree No. 19/2023).**

This situation arises when – in the event of cross-border transformations, mergers and demergers involving one or more Italian joint-stock companies and one or more joint-stock companies from another Member State that have their registered office or central administration or principal place of business established within the territory of the European Union – in order to make it appear that the conditions for issuing the preliminary certificate have been fulfilled, documents that are entirely or partially false are drawn up, genuine documents are altered, false declarations are made or relevant information is omitted.

7. The types of crimes of terrorism and subversion of the democratic order (Article 25-quater of Legislative Decree 231/01)

Art. 25-quater

Crimes with the aim of terrorism or subversion of the democratic order

((1. In relation to the commission of crimes aimed at terrorism or subversion of the democratic order, as provided for by the penal code and special laws, the following pecuniary sanctions shall apply to the entity:

a) if the crime is punishable by imprisonment of less than ten years, the pecuniary sanction is from two hundred to seven hundred shares;

b) if the crime is punishable by imprisonment of not less than ten years or by life imprisonment, the pecuniary sanction ranges from four hundred to one thousand quotas.

1. *In cases of conviction for one of the crimes indicated in paragraph 1, the disqualification sanctions provided for in Article 9, paragraph 2, shall apply for a period of no less than one year.*
2. *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 crimes indicated in paragraph 1, the sanction of permanent disqualification from exercising the activity pursuant to Article 16, paragraph 3, shall apply.*
3. *The provisions of paragraphs 1, 2 and 3 also apply in relation to the commission of crimes, other than those indicated in paragraph 1, which have in any case been committed in violation of the provisions of Article 2 of the International Convention for the Suppression of the Financing of Terrorism, concluded in New York on 9 December 1999.*

The main cases referred to in Legislative Decree 231/01 in art. 25 are briefly described below.*quarter*.

- ***Subversive associations (art. 270 of the Criminal Code)***

This provision punishes anyone who promotes, establishes, organizes, or directs associations aimed at and capable of violently subverting the economic or social order established in the State or violently suppressing the political and legal order of the State.

- ***Associations for the purpose of terrorism, including international terrorism, or subversion of the democratic order (Article 270-bis of the Criminal Code)***

This law punishes anyone who promotes, establishes, organizes, directs, or finances associations that intend to commit acts of violence for the purposes of terrorism or subversion of the democratic order.

For the purposes of criminal law, the purpose of terrorism also occurs when acts of violence are directed against a foreign state, an institution, or an international organization.

- ***Assistance to members (Article 270-ter of the Criminal Code)***

The provision in question penalises anyone who gives refuge or provides food, hospitality, means of transport, communication tools to any of the persons participating in the associations indicated in the previous articles 270 and 270-*until*.

Anyone who commits the act in favor of a close relative is not punishable.

- ***Recruitment for the purpose of terrorism, including international terrorism (Article 270-quater of the Criminal Code)***

Anyone, outside the cases referred to in the previous article 270-*until*, recruits one or more people to carry out acts of violence or sabotage essential public services, with terrorist purposes, even if directed against a foreign state, an institution or an international organization, is punishable by imprisonment from seven to fifteen years.

- ***Training for activities aimed at terrorism, including international terrorism (Article 270-quinquies of the Criminal Code)***

Anyone, outside the cases referred to in Article 270-*until* described above, trains or otherwise provides instructions on the preparation or use of explosive materials, firearms or other weapons, harmful or dangerous chemical or bacteriological substances, as well as any other technique or method for committing acts of violence or sabotage of essential public services, for terrorist purposes, even if directed against a foreign state, an institution, or an international organization, is punishable by imprisonment for five to ten years. The same penalty applies to the trained person.

- ***Conduct for the purpose of terrorism (Article 270-sexies of the Criminal Code)***

Conducts considered to have terrorist purposes are those which, by their nature or context, may cause serious damage to a country or an international organization and are carried out with the aim of intimidating the population or forcing public authorities or an international organization to perform or abstain from performing any act or destabilizing or destroying the fundamental political, constitutional, economic and social structures of a country or an international organization, as well as other conducts defined as terrorist or committed with terrorist purposes by conventions or other rules of international law binding on Italy..

- ***Attack for terrorist or subversive purposes (Article 280 of the Criminal Code)***

Anyone who, for the purposes of terrorism or subversion of the democratic order, attempts to harm a person's life or safety shall be punished under this provision.

The crime is aggravated if the acts result in very serious injury or death to the person or if the act is directed against persons exercising judicial or penitentiary functions or public safety in the exercise of or because of their functions.

- ***Act of terrorism with deadly or explosive devices (Article 280-bis of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who, for the purposes of terrorism, commits any act aimed at damaging the movable or immovable property of others through the use of explosive or other lethal devices is punishable by two to five years of imprisonment. Explosive or lethal devices are defined as weapons and similar materials listed in Article 585 of the Criminal Code and capable of causing significant property damage.

If the act is directed against the seat of the Presidency of the Republic, the Legislative Assemblies, the Constitutional Court, government bodies or in any case bodies provided for by the Constitution or by constitutional laws, the penalty is increased by up to half.

If the act results in a danger to public safety or serious damage to the national economy, the penalty is imprisonment for five to ten years.

- ***Acts of nuclear terrorism (Article 280-ter of the Criminal Code)***

Anyone who, for terrorist purposes, is punished under this provision:

- procures radioactive material for himself or others;
- creates a nuclear device or otherwise comes into possession of one.

Anyone who uses radioactive material or a nuclear device or uses or damages a nuclear facility in such a way as to release or with the concrete risk of releasing radioactive material is also punishable.

- ***Kidnapping for the purpose of terrorism or subversion (Article 289-bis of the Criminal Code)***

This criminal conduct is carried out through the kidnapping of a person for the purposes of terrorism or subversion of the democratic order.

The crime is aggravated by the death, whether intentional or unintentional, of the kidnapped person.

- ***Incitement to commit one of the crimes against the personality of the State (art. 302 of the Criminal Code)***

The law provides that anyone who incites someone to commit one of the non-negligent crimes set forth in the section of the Criminal Code dedicated to crimes against the personality of the State, for which the law establishes life imprisonment or imprisonment, is punished, if the incitement is not accepted, or if the incitement is accepted but the crime is not committed, with imprisonment from one to eight years.

- ***Political conspiracy by agreement and political conspiracy by association (Articles 304 and 305 of the Criminal Code)***

These provisions punish the conduct of anyone who agrees or associates with the aim of committing one of the crimes referred to in the previous point (art. 302 of the Criminal Code).

- ***Armed gang and its formation and participation; assistance to participants in a conspiracy or armed gang (Articles 306 and 307 of the Criminal Code)***

These crimes occur when, in order to commit one of the crimes listed in Article 302 of the Criminal Code, an armed gang is formed or shelter is given or food, hospitality, transportation, or communication tools are provided to any of the individuals participating in the indicated association or gang.

- ***Terrorist crimes provided for by special laws: these consist of all that part of Italian legislation, enacted in the 1970s and 1980s, aimed at combating terrorism.***
- ***Offences, other than those indicated in the Criminal Code and special laws, committed in violation of Article 2 of the New York Convention of 8 December 1999***

Pursuant to the aforementioned article, anyone who, by any means, directly or indirectly, illegally and intentionally, provides or collects funds with the intent to use them or knowing that they are intended to be used, in whole or in part, for the purpose of carrying out:

a) an act which constitutes a criminal offence as defined in one of the treaties listed in the Annex; or

b) any other act intended to cause death or serious physical injury to a civilian, or to any other person not taking an active part in situations of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing something.

For an act to constitute one of the aforementioned crimes, it is not necessary for the funds to actually be used to carry out what is described in letters (a) and (b).

Anyone who attempts to commit the crimes listed above also commits a crime. Anyone who:

- takes part as an accomplice in the commission of one of the above crimes;
- organizes or directs other persons to commit any of the above crimes;
- contributes to the commission of one or more of the above crimes with a group of people acting with a common purpose. Such contribution must be intentional and:
- must be carried out for the purpose of facilitating the criminal activity or purpose of the group, where such activity or purpose involves the commission of the crime; or
- must be provided with full knowledge that the group's intent is to commit a crime.

Among the criminal conducts that supplement the offences of terrorism, those that could easily be carried out are the conducts consisting in "financing" (see art. 270-*until* c.p.).

In order to determine whether or not there is a risk of committing this type of crime, it is necessary to examine the subjective profile required by the law for the purposes of determining whether the crime is constituted.

From a subjective perspective, terrorist crimes are considered intentional crimes. Therefore, for the intentional offense to occur, from the perspective of the perpetrator's psychological representation, the perpetrator must be aware of the unlawful act and intend to commit it through conduct attributable to him. Therefore, for the offenses in question to be constituted, the perpetrator must be aware of the terrorist nature of the activity and have the intent to facilitate it.

That said, for criminal conduct to constitute a crime of terrorism, the agent must be aware that the organization to which he is granting funding pursues terrorist or subversive goals and that he intends to facilitate its activities.

Furthermore, the commission of the criminal act would also be possible if the individual acted with intent. In this case, the perpetrator would have to foresee and accept the risk of the event occurring, even if he or she did not directly intend it. The foreseeable risk of the event occurring and the voluntary determination to engage in the criminal conduct must be inferred from unequivocal and objective elements.

8. The types of crimes relating to the practices of mutilation of female genital organs and crimes against the individual personality (art. 25-*quarter*. 1 e 25-quinquies of D.Lgs. 231/01)

Art. 25-quarter.1

Female genital mutilation practices

1. In relation to the commission of the crimes referred to in theArticle 583-bis of the Criminal CodeThe entity in whose structure the crime is committed is subject to a fine ranging from 300 to 700 quotas and the disqualification sanctions provided for in Article 9, paragraph 2, for a period of no less than one year. If the entity is an accredited private entity, its accreditation is also revoked.

2. If the entity or one of its organizational units is used on a permanent basis for the sole or primary purpose of enabling or facilitating the commission of the crimes indicated in paragraph 1, the sanction of permanent disqualification from exercising the activity pursuant to Article 16, paragraph 3, shall apply.

Article 25-five times

Crimes against the individual personality

1. In relation to the commission of the crimes provided for in Section I of Chapter III of Title XII of Book II of the Criminal Code, the following pecuniary sanctions shall apply to the entity:

a) for the crimes referred to in Articles 600, 601, (602 and 603-bis) the pecuniary sanction from four hundred to one thousand quotas;

b) for the crimes referred to in Articles 600-bis, first paragraph, 600-ter, first and second paragraphs, even if relating to the pornographic material referred to in Article 600-quater.1, and 600-quinquies, a pecuniary sanction of between three hundred and eight hundred quotas;

c) for the crimes referred to in Articles 600-bis, second paragraph, 600-ter, third and fourth paragraphs, and 600-quater, even if relating to the pornographic material referred to in Article 600-quater.1, as well as for the crime referred to in Article 609-undecies, a pecuniary sanction of between two hundred and seven hundred quotas.

2. In cases of conviction for one of the crimes indicated in paragraph 1, letters a) and b), the disqualification sanctions provided for in Article 9, paragraph 2, shall apply for a period of no less than one year.

3. If the entity or one of its organizational units is used on a permanent basis for the sole or primary purpose of enabling or facilitating the commission of the crimes indicated in paragraph 1, the sanction of permanent disqualification from exercising the activity pursuant to Article 16, paragraph 3, shall apply.

The main cases referred to in Legislative Decree 231/01 in art. 25 are briefly described below.*quinquies* e all'art. .

- ***Reduction or maintenance in bondage or servitude (Art. 600 c.p.)***

Whoever exercises over a person powers corresponding to those of the right of ownership, or whoever reduces or maintains a person in a state of continuous subjection, forcing him or her to perform work or sexual services or to beg or in any case to carry out illicit activities that involve his or her exploitation, or to submit to the removal of organs, is punishable by imprisonment from eight to twenty years.

Reduction or maintenance in a state of subjection occurs when the conduct is carried out through violence, threats, deception, abuse of authority or taking advantage of a situation of vulnerability, physical or mental inferiority or a situation of necessity, or through the promise or giving of sums of money or other advantages to those who have authority over the person.

- ***Underage prostitution (Art. 600-bis c.p.)***

Anyone who induces a person under the age of eighteen to engage in prostitution or who encourages or exploits prostitution is punishable by imprisonment from six to twelve years and a fine from 15,000 to 150,000 euros.

Unless the act constitutes a more serious crime, anyone who engages in sexual acts with a minor between the ages of fourteen and eighteen, in exchange for money or other financial gain, is punishable by imprisonment for one to six years and a fine of between €1,500 and €6,000.

- ***Child pornography (art. 600-ter c.p.)***

Anyone who, using minors under the age of eighteen, performs pornographic performances or produces pornographic material or induces minors under the age of eighteen to participate in pornographic performances is punishable by imprisonment for six to twelve years and a fine of between 24,000 and 240,000 euros.

Anyone who trades in the pornographic material referred to in the first paragraph is subject to the same penalty.

Anyone who, outside the cases referred to in the first and second paragraphs, by any means, including electronic means, distributes, discloses, disseminates, or advertises the pornographic material referred to in the first paragraph, or distributes or disseminates news or information aimed at the solicitation or sexual exploitation of minors under the age of eighteen, is punishable by imprisonment for one to five years and a fine of between €2,582 and €51,645.

Anyone who, outside the cases referred to in the first, second and third paragraphs, offers or transfers to others, even free of charge, the pornographic material referred to in the first

paragraph, shall be punished with imprisonment of up to three years and a fine of between €1,549 and €5,164.

In the cases provided for in the third and fourth paragraphs, the penalty is increased by no more than two thirds where the material is in large quantities.

Unless the act constitutes a more serious crime, anyone who attends pornographic performances or shows involving minors under the age of eighteen is punishable by imprisonment of up to three years and a fine of between €1,500 and €6,000.

For the purposes of this Article, child pornography means any representation, by any means, of a child under the age of eighteen engaged in explicit sexual activities, whether real or simulated, or any representation of the sexual organs of a child under the age of eighteen for sexual purposes.

- ***Possession of or access to pornographic material (Article 600-quater of the Criminal Code)***

Anyone, outside the cases provided for in Article 600-*to have*, knowingly procures or possesses pornographic material produced using minors under the age of eighteen, is punishable by imprisonment of up to three years and a fine of not less than 1,549 euros.

The penalty is increased by no more than two thirds if the material held is of a large quantity.

Except in the cases referred to in the first paragraph, anyone who, through the use of the Internet or other networks or means of communication, intentionally and without justifiable reason accesses pornographic material created using minors under the age of eighteen shall be punished with imprisonment of up to two years and a fine of not less than €1,000.

- ***Virtual pornography (art. 600-quater 1 c.p.)***

The provisions of Articles 600-*to have* and 600-*quarter*They also apply when the pornographic material represents virtual images created using images of minors under the age of eighteen or parts thereof, but the penalty is reduced by a third.

Virtual images are images created using graphic processing techniques that are not associated in whole or in part with real situations, and whose representation quality makes unreal situations appear real.

- ***Tourism initiatives aimed at exploiting child prostitution (Article 600-quinquies of the Criminal Code)***

Anyone who organizes or promotes trips aimed at the enjoyment of prostitution activities to the detriment of minors or in any case involving such activity is punishable by imprisonment from six to twelve years and a fine of between €15,493 and €154,937.

- ***Solicitation of minors (art. 609-undecies c.p.)***

Anyone who, with the aim of committing the crimes referred to in Articles 600, 600-bis, 600-*ter* and 600-*quarter*, even if relating to pornographic material as per art. 600-quater.1, 600-*quinquies*, 609-*until*, 609-*quarter*, 609-*quinquies*and 609-*octies*, entices a minor under the age of sixteen, is punished, if the act does not constitute a more serious crime, with imprisonment from one to three years.

Grooming is any act aimed at gaining the trust of a minor through trickery, flattery, or threats, including through the use of the Internet or other networks or means of communication.

The penalty is increased:

1) if the crime is committed by several people together;

2) if the crime is committed by a person who is part of a criminal association and in order to facilitate its activity;

3) if the act, due to the repetition of the conduct, causes serious harm to the minor;

4) if the act results in danger to the minor's life.

- ***Human trafficking (Article 601 of the Criminal Code)***

Whoever commits trafficking in a person who is in the conditions referred to in Article 600 or, in order to commit the crimes referred to in the same Article, induces that person by deception or forces that person by violence, threats, abuse of authority or of a situation of physical or mental inferiority or of a situation of necessity, or by promising or giving sums of money or other benefits to the person who has authority over them, to enter, reside in, or leave the territory of the State or to move within it, is punishable by imprisonment from eight to twenty years.

- ***Purchase and sale of slaves (Article 602 of the Criminal Code)***

Whoever, outside the cases indicated in Article 601, acquires or sells or transfers a person who is in one of the conditions referred to in Article 600 is punishable by imprisonment from eight to twenty years.

- ***Illegal intermediation and exploitation of labor (Article 603-bis of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who:

1) recruits workers for the purpose of assigning them to work for third parties in exploitative conditions, taking advantage of the workers' state of need;

2) uses, hires or employs labour, including through the intermediation activity referred to in number 1), subjecting workers to exploitative conditions and taking advantage of their state of need.

If the acts are committed through violence or threats, the penalty is five to eight years of imprisonment and a fine of €1,000 to €2,000 for each worker recruited.

For the purposes of this article, the existence of one or more of the following conditions constitutes an indication of exploitation:

1) the repeated payment of wages in a manner that is clearly different from the national or territorial collective agreements stipulated by the most representative trade union organizations at the national level, or in any case disproportionate to the quantity and quality of the work performed;

2) repeated violation of the regulations relating to working hours, rest periods, weekly rest, compulsory leave, and holidays;
3) the existence of violations of the regulations regarding safety and hygiene in the workplace;
4) subjecting the worker to degrading working conditions, surveillance methods or housing situations.
5) They constitute a specific aggravating circumstance and lead to an increase in the penalty by one third to one half:

    a) the fact that the number of workers recruited is greater than three;

    b) the fact that one or more of the recruited subjects are minors of non-working age;

    c) having committed the act by exposing the exploited workers to situations of grave danger, taking into account the characteristics of the tasks to be performed and the working conditions.

- ***Female genital mutilation (Article 583 bis of the Criminal Code)***

Anyone who, without therapeutic need, causes female genital mutilation shall be punished with four to twelve years of imprisonment. For the purposes of this article, female genital mutilation shall be defined as clitoridectomy, excision, infibulation, and any other practice that causes similar effects. Anyone who, without therapeutic need, causes, for the purpose of impairing sexual function, injuries to the female genital organs other than those indicated in the first paragraph, resulting in physical or mental illness, shall be punished with three to seven years of imprisonment.

The penalty is reduced by up to two thirds if the injury is minor.

The penalty is increased by one-third when the practices referred to in the first and second paragraphs are committed against a minor or if the act is committed for profit. The provisions of this article also apply when the act is committed abroad by an Italian citizen or a foreigner resident in Italy, or against an Italian citizen or a foreigner resident in Italy. In this case, the offender is punished at the request of the Minister of Justice.

With regard to crimes related to slavery, these criminal hypotheses extend not only to the individual who directly carries out the illicit act, but also to anyone who knowingly facilitates the same conduct, even financially.

The relevant conduct in these cases may be the illegal procurement of labor through migrant smuggling and the slave trade.

9. The types of administrative crimes and offences of market *abuse* (art. 25 *sexies* of Legislative Decree 231/2001

9.1 Administrative crimes and offenses

The criminal and administrative offences of market abuse are regulated by the new Title I-*until*, Chapter II, Part V of Legislative Decree 24 February 1998, n. 58 (Consolidated Finance Act, "TUF") entitled “Abuse of privileged information and market manipulation”.

According to the new regulation, in fact, the entity may be held liable both when crimes of abuse of privileged information (art. 184 TUF) or market manipulation (art. 185 TUF) are committed in its interest or to its advantage, and when the same conduct does not constitute crimes but simple administrative offences (respectively art. 187 –*until* TUF for the abuse of privileged information and 187 -*to have* TUF for market manipulation).

Art. 25-sexies

Market abuse

1. In relation to the crimes of insider trading and market manipulation provided for in Part V, Title I-bis, Chapter II, of the consolidated text referred to in Legislative Decree no. 58 of 24 February 1998, the entity shall be subject to a pecuniary sanction ranging from four hundred to one thousand shares.

2. If, following the commission of the crimes referred to in paragraph 1, the product or profit obtained by the entity is of a significant amount, the sanction is increased up to ten times such product or profit)

In the event that the unlawful conduct constitutes the crime, the entity's liability will be based on Article 25.*sexies*of Legislative Decree 231/01; if, on the contrary, the offence is to be classified as administrative, the entity will be liable *ex* art. 187– *quinquies*TU

- ***Abuse of privileged information (art. 184 TUF)***

Anyone who, having directly come into possession of inside information through being a member of the administrative, management or control bodies of an issuing company, or through being a shareholder of the latter, or through having learned such information in the course of and as a result of a private or public work activity, commits the crime of insider dealing:

- buys, sells or carries out other transactions, directly or indirectly, on its own account or on behalf of third parties, on financial instruments[5]using the privileged information acquired in the ways described above;

[5]"Financial instruments" means:
(1) transferable securities; (2) money market instruments; (3) units in a collective investment undertaking; (4) options contracts, futures, swaps, interest rate agreements and other derivative contracts relating to transferable securities, currencies, interest rates or yields, emission allowances or other derivative financial instruments, financial indices or financial measures which can be settled by physical delivery of the underlying asset or by payment of differentials in cash; (5) options contracts, futures, swaps, forwards and other derivative contracts relating to commodities where settlement must take place by payment of differentials in cash or can take place in cash at the option of one of the parties, except where such option follows a default or other event which determines the termination of the contract; (6) options, futures, swaps and other derivative contracts relating to commodities which can be settled by physical delivery provided they are traded on a regulated

- communicates such information to others, outside the normal exercise of his work, profession, function or office (regardless of whether those who receive such information use it to carry out transactions) or a market survey carried out pursuant to Article 11 of Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014;
- recommends or induces others, on the basis of privileged information in his possession, to carry out any of the operations indicated in the first point.

Furthermore, the crime of abuse of privileged information is committed by anyone who, having come into possession of privileged information due to the preparation or execution of criminal activities, carries out any of the actions mentioned above (this is the case, for example, of the "computer hacker" who, following unauthorised access to a company's computer system, manages to come into possession of confidential information).*price sensitive*).

The crime in question is also committed by anyone who, being in possession of privileged information for reasons other than those indicated above and knowing the privileged nature of such information, commits any of the actions indicated above.

Example:
The company's Finance Manager issues orders to buy and sell shares of a listed company (for example, a*partner* commercial company) based on inside information.

- ***Market manipulation (art. 185 TUF)***

Anyone who spreads false information (so-called information manipulation) or carries out simulated transactions or other artifices concretely capable of causing a significant alteration in the price of financial instruments (so-called trading manipulation) commits the crime of market manipulation.

---

market, a multilateral trading facility or an organised trading facility, except for wholesale energy products traded on an organised trading facility which must be settled by physical delivery; (7) options, futures, swaps, forwards and other derivative contracts relating to commodities which cannot be executed in ways other than those referred to in point 6, which are not for commercial purposes, and which have the characteristics of other derivative financial instruments; (8) Derivative financial instruments for the transfer of credit risk; (9) contracts for difference; (10) options contracts, futures, swaps, interest rate forward contracts and other derivative contracts relating to climatic variables, freight tariffs, inflation rates or other official economic statistics, where settlement is by cash settlement or may be settled at the discretion of one of the parties, except where such discretion follows a default or other termination event, as well as other derivative contracts relating to assets, rights, obligations, indices and measures, not otherwise specified in this Section, having the characteristics of other derivative financial instruments, having regard, inter alia, to whether they are traded on a regulated market, a multilateral trading facility or an organised trading facility; (11) emission allowances consisting of any recognised unit complying with the requirements of Directive 2003/87/EC (Emissions Trading Scheme).

With reference to the dissemination of false or misleading information, it is also emphasized that this type of market manipulation also includes cases in which the creation of a misleading indication arises from the failure to comply with disclosure obligations by the issuer or other obligated parties.

Examples:

The General Manager of the company spreads false communications about corporate events (for example about the existence of ongoing restructuring projects) or about the situation of the company with the aim of influencing the prices of listed securities (*information manipulation*).

The Finance Manager issues buy and sell orders relating to one or more specific financial instruments or derivative contracts close to the end of trading in order to alter their final price (*negotiation manipulation*).

Furthermore, with reference to the examples reported, it is emphasized that the entity's liability can only be established if such behaviors were carried out in its interest or to its advantage by persons holding representative, administrative, or management roles within the entity itself or within one of its organizational units with financial and functional autonomy, as well as by persons who exercise, even de facto, management and control over the entity itself, or by persons subject to the direction or supervision of one of the aforementioned entities.

Administrative offenses:

- ***Abuse of privileged information (Article 187-bis of the TUF)***

Anyone who violates the prohibition of insider dealing and unlawful disclosure of inside information pursuant to Article 14 of Regulation (EU) No. 596/2014 (the "**MAR Regulation**").

The offense covered by this article largely corresponds to the criminal offense governed by Article 184 of the TUF, differing primarily in the absence of intent in the unlawful conduct (a necessary condition, however, for the offense of insider dealing to be constituted). In order for the administrative offense of insider dealing to be constituted, it is sufficient that the conduct be negligent, and the actual intent of the perpetrator of the offense is therefore irrelevant.

Finally, it should be emphasized that for the cases provided for in the article in question, the attempt is equivalent to consummation.

Example:

The Manager*Merger & Acquisition* negligently (with a careless attitude) induces others to carry out transactions on financial instruments on the basis of privileged information acquired in the exercise of his function.

- ***Market manipulation (art. 187-ter TUF)***

The situation provided for by art. 187-*to have* The TUF punishes (without prejudice to criminal sanctions when the act constitutes a crime) anyone who violates the prohibition on

market manipulation pursuant to Article 15 of the MAR Regulation with an administrative pecuniary sanction ranging from twenty thousand euros to five million.

Example:

The Manager*Investor Relations* disseminates false or misleading information through the press with the intention of moving the price of a security or underlying asset in a direction that favors the open position on that financial instrument or asset or favors a transaction already planned by the person disseminating the information.

9.2. The concept of Inside Information

The concept of privileged information represents the fulcrum around which the entire discipline on the subject revolves.*insider trading* and that concerning corporate information regulated in Title III, Chapter I, art. 114 et seq. of the TUF and in Consob Regulation no. 11971/1999 (hereinafter the "Issuers Regulation").

According to the provisions of art. 7 MAR (to which art. 180, paragraph 1, letter b) refers to *have*), of the TUF), information **is to be considered privileged**(hereinafter the **"Insider Information**"):

- **of a precise nature**: that is, information relating to circumstances or events that exist or have occurred, or to circumstances or events that can reasonably be expected to come into existence or occur; furthermore, it must be sufficiently explicit and detailed information so that whoever uses it is placed in a position to believe that its use may actually have certain effects on the price of financial instruments, even if, possibly, it is "progressively formed";
- **not yet made public**: that is, information not yet made available to the market, for example through publication on websites or in newspapers or through communications made to Supervisory Authorities;
- **relating, directly or indirectly, to one or more issuers of financial instruments or one or more financial instruments**: that is, so-called "corporate information", i.e. information relating to the economic, financial or organizational situation of the issuer, or so-called "market information", i.e. information relating to the events of one or more financial instruments.
- **which, if made public, could significantly affect the prices of such financial instruments or the prices of related derivative financial instruments**: that is, information that presumably a reasonable investor (average investor) would use as one of the elements on which to base his investment decisions.

Finally, it should be emphasized that for information to be considered privileged, all of the characteristics described above must be present, with the absence of just one of them being sufficient to deprive the information of its privileged nature.

9.3. Information obligations

The implementation of EU legislation on market abuse has brought significant innovations to the information system required for listed companies.

Consob has amended the Issuers' Regulations by establishing new rules regarding:

- **the communication to the public of information relating to transactions onfinancial instruments carried out by "persons exercising administrative, control or management functions, as well as by relevant persons and persons closely linked to them**". The disclosure obligations required pursuant to art. 114 of the TUF for the following entities are summarized below:

- listed issuers and the entities that control them;
- members of the administrative and control bodies;
- managers;
- entities holding a significant shareholding pursuant to Article 120 of the TUF (i.e., those holding more than two percent of the capital of a listed company and listed companies holding more than ten percent of the capital of an unlisted company);

- entities participating in an agreement provided for by art. 122 of the TUF (i.e., a shareholders' agreement concerning the exercise of voting rights in listed companies and in the companies that control them);

- Persons closely related to relevant persons are understood to be:
    - the spouse if not legally separated, the dependent children, including the spouse's children, and, if they have been living together for at least a year, the parents, relatives and in-laws of the relevant persons;
    - legal entities, partnerships and trusts in which a relevant person or one of the persons indicated above holds, alone or jointly, the management function;
    - legal entities, directly or indirectly controlled by a relevant person or by one of the persons indicated in the first point;
    - partnerships whose economic interests are substantially equivalent to those of a relevant person or one of the persons indicated in the first point;
    - i *trust established* for the benefit of a relevant person or one of the natural persons indicated in the first point;

- **the new regulation regarding the communication to the public of information relating to to transactions on financial instruments carried out by relevant persons provides** that:

- Persons performing administrative, control or management functions in a listed issuer or in a significant subsidiary, the managers of the issuer, or of a significant subsidiary, who have regular access to the Inside Information referred to in Article 181 of the TUF and hold the power to adopt management decisions that may affect the development and future prospects of the listed issuer, must communicate to Consob and publish the transactions in shares and related financial instruments carried out by themselves (and by persons closely associated with them).[6]) by the

[6]By "persons closely related to relevant persons" we mean:

end of the fifteenth day of the month following the month in which the transaction was carried out. The listed issuer will therefore be required to communicate the information to the public by the end of the trading day following the day of receipt (Article 152–octies, paragraphs 1, 2, and 3, Issuers' Regulations);

- the entities holding at least 10 percent of the share capital, as well as any other entity controlling the listed issuer, having the right to vote of the listed issuer must communicate any relevant transactions pursuant to the provisions on *internal dealing* to Consob and then disclose the information to the public by the end of the fifteenth day of the month following the month in which the transaction was carried out. They may, however, delegate the issuer to publish the information to the public. The listed issuer will then be required to disclose the information to the public by the end of the trading day following the day of receipt.

The Issuers' Regulation extends the aforementioned obligations to the purchase, sale, subscription or exchange of shares or financial instruments linked to shares (Article 152–septies, paragraph 2).

The following transactions carried out by relevant persons and closely related persons are exempt from the reporting obligation:

- transactions whose total amount does not reach twenty thousand euros by the end of the year; after each communication, transactions whose total amount does not reach a value of further
- twenty thousand euros by the end of the year; for related derivative financial instruments, the amount is calculated with reference to the underlying shares;
- transactions that are carried out between the relevant person and persons closely associated with him;
- transactions carried out by the listed issuer itself and by companies controlled by it;
- transactions carried out by a credit institution or an investment firm which contribute to the formation of the trading book of that institution or firm, as defined in Article 4, paragraph 1, point 86, of Regulation (EU) No 575/2013, provided that the same entity:
    - keep the negotiation and management structures organizationally separate from the treasury and the structures that manage strategic holdings/market *making*;
    - be able to identify the shares held for trading purposes and/or market *making*, through methods that can be subject to verification by Consob, or by holding them in a specific separate account;

and, if you act as market *maker*,

- is authorised by the Member State of origin pursuant to Directive 2014/65/EU to carry out the activity of *market making*;
- provide Consob with the agreement *market making with* the market operator and/or with the issuer where required by law and the relevant implementing

provisions in force in the EU Member State where the*market maker*carries out its activity;

- notify Consob that it intends to carry out or carries out activities of *market making on* the shares of a listed issuer of shares, using the TR-2 form contained in Annex 4;*market maker* must also notify Consob without delay of the cessation of the activity of *market making on* the same actions.

- **<u>public disclosure of Inside Information</u>**

The new regulation regarding the public disclosure of Inside Information provides that:

- The disclosure obligations set forth in Article 114 of the TUF for listed issuers and the entities that control them (hereinafter "the Obliged Parties") concerning Inside Information that directly concerns the issuer and its subsidiaries, are fulfilled when a set of circumstances or an event occurs "*although not yet formalized*", the public was informed without delay (art. 17 MAR).

The publication of such information must take place through a specific press release distributed in the manner indicated in Chapter I in relation to the dissemination of regulated information.

The issuer must also publish the press release on its website, where available, and keep it there for at least five years (Article 17, MAR Regulation).

Listed issuers shall issue the necessary instructions so that their subsidiaries provide all the information required to comply with the disclosure obligations required by law. Subsidiaries shall promptly provide the requested information.

Inside Information and marketing the activities of the Obliged Parties must not be combined with each other in a way that is misleading (art. 17 MAR)

Obliged Parties must fully disclose to the public any Inside Information that, intentionally or unintentionally, they have disclosed in the course of their work, profession, function, or office to third parties not subject to any confidentiality obligation (Article 17, paragraph 8, MAR). Furthermore, when, following the disclosure of information concerning the financial, economic, or financial situation of issuers of financial instruments, or extraordinary financial transactions relating to such issuers, the price of those instruments changes compared to the last price of the previous day, Obliged Parties must publish, in the prescribed manner, a statement confirming the accuracy of the information, supplementing or correcting its content, in order to restore equal information (Article 66, paragraph 8, Issuers' Regulation).

Obliged Parties have the right to delay disclosing Inside Information to the market in order not to prejudice their legitimate interests (Article 17, paragraph 5 of the MAR). Relevant circumstances that justify this right are those in which the public disclosure of Inside Information could jeopardize the execution of a transaction by the issuer itself or give rise to incomplete assessments by the public.

The Obliged Parties who avail themselves of the delay in communication must observe the procedures necessary and suitable to guarantee the confidentiality of the information and communicate the Privileged Information without delay when such confidentiality should cease to exist (art. 66-*until* paragraph 3, Issuers' Regulation). These entities are required to communicate the delay and the reasons therefor to Consob without delay (art. 66-*until* (Section 4 of the Issuers' Regulations). Following such communication or having otherwise received notice of a delay in public disclosure of Inside Information, Consob may require the interested parties to proceed with the communication and, in the event of non-compliance, pay the costs at the interested parties' expense.

Consob may, even on a general basis, require Obliged Parties, members of the administrative and supervisory bodies, and managers, as well as persons who hold a significant shareholding pursuant to Article 120 of the TUF (i.e., those who hold more than two percent of the capital of a listed company and listed companies that hold more than ten percent of the capital of an unlisted company) or who participate in an agreement pursuant to Article 122 of the TUF (i.e., a shareholders' agreement concerning the exercise of voting rights in listed companies and their parent companies) to disclose, in accordance with the procedures established by Consob, the information and documents necessary for public information.

In case of non-compliance, the Authority may proceed directly at the expense of the defaulting party (Article 114, paragraph 5, TUF).

10. The crimes of manslaughter and serious or very serious bodily harm committed in violation of accident prevention and occupational health and hygiene regulations (Article 25-septies of Legislative Decree 231/01 - Legislative Decree no. 81 of 9 April 2008)

Article 9 of Law no. 123 of 3 August 2007 amended Legislative Decree 231/01 by introducing the new Article 25-*septies* which extends the liability of entities to crimes related to the violation of safety and accident prevention regulations.
Pursuant to Article 1 of Law 123/07, Legislative Decree no. 81 of 9 April 2008 regarding health and safety in the workplace came into force.

This provision is a Consolidated Law coordinating and harmonizing all existing laws on the matter, with the intention of creating a single, easy-to-use instrument for all those involved in safety management.

In particular, Legislative Decree 81/2008 repeals several important safety regulations, including Legislative Decree 626/94 (Implementation of EU directives on improving the safety and health of workers at work), Legislative Decree 494/96 (Implementation of the EU directive on the minimum safety and health requirements for temporary or mobile construction sites), and, lastly, Articles 2, 3, 4, 5, 6, and 7 of Law 123/2007.

Article 300 of Legislative Decree 81/2008 replaced the wording of Article 25-*septies* of the aforementioned Legislative Decree 231/01, referring to the crimes referred to in Articles 589 (culpable homicide) and 590, paragraph 3 (serious or very serious personal injury through

negligence) of the Criminal Code, committed in violation of accident prevention and workplace health and hygiene regulations.

Art. 25-septies

Manslaughter or serious or very serious injury committed in violation of the regulations on health and safety at work

1. In relation to the crime referred to in Article 589 of the Criminal Code, committed in violation of Article 55, paragraph 2, of the Legislative Decree implementing the delegation pursuant to Law No. 123 of August 3, 2007, regarding occupational health and safety, a fine of 1,000 quotas shall apply. In the event of a conviction for the crime referred to in the previous sentence, the disqualification sanctions referred to in Article 9, paragraph 2, shall apply for a period of no less than three months and no more than one year.

2. Except as provided in paragraph 1, in relation to the crime referred to in Article 589 of the Criminal Code, committed in violation of the regulations on occupational health and safety, a pecuniary sanction of no less than 250 quotas and no more than 500 quotas shall apply. In the event of a conviction for the crime referred to in the previous sentence, the disqualification sanctions referred to in Article 9, paragraph 2, shall apply for a period of no less than three months and no more than one year.

3. In relation to the crime referred to in Article 590, paragraph 3, of the Criminal Code, committed in violation of the regulations on health and safety at work, a pecuniary sanction of no more than 250 quotas shall apply. In the event of a conviction for the crime referred to in the previous sentence, the disqualification sanctions referred to in Article 9, paragraph 2, shall apply for a period of no more than six months.

The new wording has redefined the sanctions applicable to the entity, grading them in relation to the crime and the aggravating circumstances that may arise in its commission.

- ***Manslaughter (art. 589 of the Criminal Code)***

The crime occurs whenever a person negligently causes the death of another person.

However, the criminal offence included in Legislative Decree 231/01 concerns only those cases in which the death was caused not by general fault, and therefore by incompetence, imprudence or negligence, but by specific fault, consisting in the violation of the regulations for the prevention of accidents at work.

In relation to the crime in question, the new art. 25-*seven times*Legislative Decree 231/01 provides for a fine of one thousand quotas and a disqualification from three months to one year, but only when this is committed in violation of art. 55, paragraph 2 of the Consolidated Law, that is, when the criminal conduct is committed within certain specific types of companies (i.e., industrial companies with more than 200 employees or those in which workers are exposed to biological risks, asbestos, etc.).

However, if the same crime is committed simply by violating accident prevention regulations, a fine of 250 to 500 quotas applies, while in the event of a conviction for such a crime, a disqualification sanction of three months to one year applies.

- ***Serious or very serious personal injury through negligence (art. 590 c. 3 c.p.)***
The crime occurs whenever a person, in violation of the regulations for the prevention of accidents at work, causes serious or very serious injuries to another person.

Pursuant to paragraph 1 of art. 583 of the Criminal Code, the injury is considered grave in the following cases:

"1) if the act results in an illness that endangers the life of the injured party, or an illness or inability to carry out ordinary activities for a period exceeding forty days;

2) if the fact causes the permanent weakening of a sense or an organ".

Pursuant to paragraph 2 of art. 583 of the Criminal Code, the injury is instead considered very serious if the fact results in:

- *"a disease that is certainly or probably incurable;*
- *the loss of a sense;*
- *the loss of a limb, or a mutilation that renders the limb useless, or the loss of the use of an organ or the ability to procreate, or a permanent and serious difficulty in speaking."*

If the crime in question is committed in violation of accident prevention regulations, the entity will be subject to a fine of no more than 250 quotas and, in the event of a conviction for such crime, a disqualification sanction of up to six months will be applied.

In any case, Article 5 of Legislative Decree 231/01 requires that the crimes were committed in the interest of the entity or to its advantage.

Legislative Decree 81/2008 also provides in Article 30 that, in order to avoid the entity's administrative liability, the Organization, Management and Control Model pursuant to Legislative Decree 231/01 must be adopted and effectively implemented, ensuring compliance with specific legal obligations, specifically relating to:

- compliance with the legal technical-structural standards relating to systems, workplaces and work equipment;
- to risk assessment activities and the preparation of the resulting prevention and protection measures;
- to organizational activities (i.e. first aid, contract management, periodic safety meetings, consultations with workers' safety representatives);
- to worker information and training activities, as well as health surveillance;
- to supervisory activities, with reference to workers' compliance with safety procedures and instructions;
- to the acquisition of legally required documentation and certifications;
- to periodic checks on the application and effectiveness of the procedures adopted.

11. The offences of receiving, laundering and using money, goods or utilities of illicit origin, as well as self-laundering (art. 25-*octies*D.Lgs. 231/01 - D.Lgs. 231/2007)

Legislative Decree 231/2007, also known as the "Anti-Money Laundering Decree" (which implemented Directive 2005/60/EC for 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 which contains implementing measures), has inserted the new art. 25 into the body of Legislative Decree 231/01.*octies*, which extends the liability of legal persons to the crimes of receiving stolen goods, money laundering and use of money, goods or utilities of illicit origin (articles 648, 648-bis and 648-ter of the Criminal Code), even if committed at the national level.

Law 146/2006 (paragraphs 5 and 6 of Article 10, now repealed by the Anti-Money Laundering Decree) had already established the liability of entities only for the crimes of money laundering and the use of money, goods, or utilities of illicit origin, and only when these were committed on a transnational level.

The crimes of receiving stolen goods, money laundering, and using money, goods, or utilities of illicit origin are considered such even if the activities that generated the assets to be laundered took place in the territory of another EU Member State or a third country.

The purpose of Decree 231/2007 is therefore to protect the financial system from being used for money laundering or terrorist financing purposes and is aimed at a group of entities that includes, in addition to banks and financial intermediaries, all those operators who carry out activities such as the custody and transportation of cash, securities, real estate brokerage agencies, etc., (the so-called "non-financial operators").

Article 25-*octies*It was amended by Law No. 186 of 15 December 2014, containing "Provisions regarding the disclosure and repatriation of capital held abroad as well as for strengthening the fight against tax evasion. Provisions regarding self-laundering", which introduced the crime of self-laundering (Article 648-ter.1 of the Criminal Code).

Art. 25-octies

Receiving, laundering and use of money, goods or utilities of illicit origin (as well as self-laundering)

1. In relation to the crimes referred to in Articles 648, 648-bis (648-ter, and 648-ter.1) of the Criminal Code, a fine ranging from 200 to 800 shares applies to the entity. If the money, goods, or other benefits derive from a crime carrying a maximum prison sentence of more than five years, a fine ranging from 400 to 1,000 shares applies.

2. In cases of conviction for one of the crimes referred to in paragraph 1, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity for a period not exceeding two years.

3. In relation to the offenses referred to in paragraphs 1 and 2, the Ministry of Justice, after consulting the UIF, formulates the observations referred to in Article 6 of Legislative Decree no. 231 of 8 June 2001.

- ***Receiving stolen goods (art. 648 of the Criminal Code)***

This crime occurs when, outside of cases of complicity in the crime, a person, for the purpose of obtaining a profit for himself or others, purchases, receives, or conceals money or property derived from any crime, or otherwise interferes in the purchase, receipt, or concealment of such property. This offense is punishable by imprisonment from two to eight years and a fine from €516 to €10,329.

The penalty is imprisonment from one to four years and a fine from €300 to €6,000 when the act involves money or property derived from a contravention punishable by imprisonment for a maximum of one year or a minimum of six months.

The penalty is increased if the act is committed in the exercise of a professional activity.

If the offense is particularly minor, the penalty is up to six years of imprisonment and a fine of up to €1,000 in the case of money or property derived from crime, and up to three years of imprisonment and a fine of up to €800 in the case of money or property derived from a contravention.

The provisions of this article also apply when the perpetrator of the crime, from whom the money or things come, is not accountable or punishable or when a condition for prosecution relating to that crime is missing.

- ***Money laundering (art. 648-bis of the Criminal Code)***

This crime occurs when a person substitutes or transfers money, goods, or other assets derived from crime, or carries out other transactions related to them, in a manner that hinders the identification of their criminal origin. This offense is punishable by imprisonment for four to twelve years and a fine of €5,000 to €25,000.

The penalty is imprisonment from two to six years and a fine from €2,500 to €12,500 when the act involves money or property derived from a contravention punishable by imprisonment for a maximum of one year or a minimum of six months.

The penalty is increased when the act is committed in the exercise of a professional activity.

The penalty is reduced if the money, goods or other benefits come from a crime for which the maximum prison sentence is less than five years.

- ***Use of money, goods or utilities of illicit origin (Article 648-ter of the Criminal Code)***

This crime occurs when money, goods, or other benefits derived from crime are used in economic or financial activities. This offense carries a prison sentence of four to twelve years and a fine of €5,000 to €25,000. The penalty is increased when the offense is committed in the exercise of a professional activity.

The penalty is imprisonment from two to six years and a fine from €2,500 to €12,500 when the act involves money or property derived from a contravention punishable by imprisonment for a maximum of one year or a minimum of six months.

The penalty is increased when the act is committed in the exercise of a professional activity.

The penalty is reduced if the act is particularly trivial.

- ***Self-laundering (art. 648-ter. 1 c.p.)***

A prison sentence of two to eight years and a fine of €5,000 to €25,000 shall apply to anyone who, having committed or aided in the commission of a non-negligent crime, uses, substitutes, or transfers, in economic, financial, entrepreneurial, or speculative activities, money, goods, or other benefits deriving from the commission of that crime, in such a way as to concretely hinder the identification of their criminal origin.

The penalty is one to four years of imprisonment and a fine of €2,500 to €12,500 when the act involves money or property derived from a contravention punishable by a maximum imprisonment of one year or a minimum of six months.

The penalty is reduced if the money, goods or other benefits derive from the commission of a crime punishable by a maximum prison term of less than five years.

In any case, the penalties set forth in the first paragraph shall apply if the money, goods, or other benefits derive from a crime committed under the conditions or for the purposes set forth in Article 7 of Legislative Decree No. 152 of May 13, 1991, converted, with amendments, by Law No. 203 of July 12, 1991, and subsequent amendments.

Except for the cases referred to in the previous paragraphs, conduct whereby money, goods or other utilities are used merely for personal use or enjoyment is not punishable.

The penalty is increased when the acts are committed in the exercise of a banking or financial activity or other professional activity.

The penalty is reduced by up to half for those who have effectively worked to prevent the conduct from leading to further consequences or to ensure evidence of the crime and the identification of the goods, money and other benefits deriving from the crime.

The last paragraph of Article 648 applies.

Pursuant to art. 25-*octies*Therefore, pecuniary sanctions of up to a maximum of 1,500,000 euros and interdictory sanctions of no more than two years may be applied to the entity in the event of the commission of one of the crimes referred to in this article, even if committed on a purely national level, provided that this results in an interest or advantage for the entity itself.

The powers and functions of the Supervisory Body have been redesigned. Its task, pursuant to Legislative Decree 231/01, is to oversee the implementation of the Organization, Management and Control Models.

12. matter of payment instruments other than cash (art. 25-*octies*.1 D.Lgs. 231/01)

Art. 25-octies.1

Crimes relating to non-cash payment instruments

1. In relation to the commission of crimes provided for by the Criminal Code regarding non-cash payment instruments, the following pecuniary sanctions apply to the entity:

a) for the crime referred to in Article 493-ter, a pecuniary sanction ranging from 300 to 800 quotas;

b) for the crime referred to in Article 493-quater and for the crime referred to in Article 640-ter, in the case aggravated by the transfer of money, monetary value or virtual currency, a pecuniary sanction of up to 500 shares.

2. Unless the act constitutes another administrative offence punishable more severely, in relation to the commission of any other crime against public trust, against property or which in any way offends the property provided for by the Criminal Code, when it involves payment instruments other than cash, the following pecuniary sanctions shall apply to the entity:

a) if the crime is punishable by imprisonment of less than ten years, a pecuniary sanction of up to 500 quotas;

b) if the crime is punishable by a sentence of not less than ten years of imprisonment, a pecuniary sanction of between 300 and 800 quotas.

2 bis. In relation to the commission of the crime referred to in Article 512 bis of the Criminal Code, the entity is subject to a pecuniary sanction ranging from 250 to 600 quotas.

3. In cases of conviction for one of the crimes referred to in paragraphs 1 and 2, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity.

The individual cases covered by the law are described below:

- *Improper use and counterfeiting of payment instruments other than cash (Art. 493-*to have *c.p.)*

Anyone who, for the purpose of profiting for themselves or others, unlawfully uses credit or payment cards, or any other similar document that authorizes the withdrawal of cash or the purchase of goods or the provision of services, or any other non-cash payment instrument, without being their owner, is punishable by imprisonment for one to five years and a fine of €310 to €1,550. The same penalty applies to anyone who, for the purpose of profiting for themselves or others, falsifies or alters the instruments or documents referred to in the first sentence, or possesses, transfers, or acquires such instruments or documents of illicit origin or otherwise falsified or altered, as well as payment orders produced with them.

In the event of a conviction or application of the penalty at the request of the parties pursuant to Article 444 of the Code of Criminal Procedure for the crime referred to in the first paragraph, the confiscation of the things that were used or intended to commit the crime, as well as of the profit or product, unless they belong to a person not involved in the crime, is ordered, or when this is not possible, the confiscation of goods, sums of money and other utilities available to the offender for a value corresponding to such profit or product.

The instruments seized for the purposes of confiscation referred to in the second paragraph, during judicial police operations, are entrusted by the judicial authority to the police bodies that request them.

- Possession and distribution of equipment, devices or computer programs aimed at committing crimes involving payment instruments other than cash (Art. 493-quarter c.p.)

Unless the act constitutes a more serious crime, anyone who, for the purpose of using them or allowing others to use them in the commission of crimes involving payment instruments other than cash, produces, imports, exports, sells, transports, distributes, makes available, or in any way procures for himself or others equipment, devices, or computer programs that, due to their technical, construction, or design characteristics, are primarily designed to commit such crimes, or are specifically adapted for the same purpose, is punishable by imprisonment of up to two years and a fine of up to €1,000.

In the event of a conviction or application of the penalty at the request of the parties pursuant to Article 444 of the Code of Criminal Procedure for the crime referred to in the first paragraph, the confiscation of the aforementioned equipment, devices or computer programs shall always be ordered, as well as the confiscation of the profits or products of the crime or, when this is not possible, the confiscation of goods, sums of money and other utilities available to the offender for a value corresponding to such profits or products.

- Frode informatica (Art. 640-to have c.p.)

For the description of art. 640-*to have*c.p., please refer to the information set out in point 1 of this Annex. It is specified that art. 25-*octies*.1 of Legislative Decree 231/2001 provides for the relevance of the above-mentioned offence only in the aggravated case referred to in the second paragraph of art. 640-*to have* c.p. ("*if the act results in a transfer of money, monetary value or virtual currency or is committed by abusing the status of system operator*").

- Fraudulent transfer of assets (Art. 512 bis of the Criminal Code)

Unless the act constitutes a more serious crime, anyone who fictitiously attributes to others the ownership or availability of money, goods or other utilities for the purpose of evading the provisions of the law regarding patrimonial or smuggling prevention measures, or of facilitating the commission of one of the crimes referred to in Articles 648, 648 bis and 648 ter, shall be punished with imprisonment from two to six years.

The same penalty referred to in the first paragraph applies to anyone who, in order to evade the provisions regarding anti-mafia documentation, fictitiously attributes to others the ownership of businesses, company shares or stocks or corporate positions, if the entrepreneur or company participates in procedures for the awarding or execution of contracts or concessions.

13. Crimes relating to infringement of copyright (art. 25-*novies* D.Lgs. 231/01)

Law no. 99 of 23 July 2009, art. 15, paragraph 7, introduced the crimes of copyright infringement into art. 25-novies of Legislative Decree 231/01.

Article 25-nine
Copyright infringement crimes

1. In relation to the commission of the crimes provided for in Articles 171, first paragraph, letter a-bis), and third paragraph, 171-bis, 171-ter, 171-septies and 171-octies of Law No. 633 of 22 April 1941, a pecuniary sanction of up to five hundred quotas shall apply to the entity.

2. In the event of a conviction for the crimes referred to in paragraph 1, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity for a period not exceeding one year. The provisions of Article 174-quinquies of the aforementioned Law No. 633 of 1941 shall remain unchanged. (17) ((20))

The individual cases covered by the law are described below:

- ***Art. 171 (1st paragraph, letter a-bis) and 3rd paragraph (L.633/1941)***

Except as provided in Article 171-*until* and from Article 171-*to have* Anyone who, without being entitled to do so, for any purpose and in any form, shall be punished with a fine ranging from €51.00 to €2,065.00:
a *until*) makes a protected intellectual work, or part of it, available to the public by placing it in a telematic network system, through connections of any kind;

The penalty is imprisonment of up to one year or a fine of not less than €516.00 if the above-mentioned crimes are committed on another's work not intended for publication, or by usurping authorship of the work, or by deformation, mutilation or other modification of the work itself, if this results in an offence to the author's honour or reputation.

- ***Art. 171-bis (L.633/1941)***

Anyone who unlawfully duplicates, for profit, computer programs, or for the same purposes imports, distributes, sells, possesses for commercial or business purposes, or leases programs contained on media not marked pursuant to this law, is subject to imprisonment from six months to three years and a fine of between five million and thirty million lire. The same penalty applies if the offense involves any means intended solely to allow or facilitate the arbitrary removal or functional circumvention of devices applied to protect a computer program. The penalty is not less than a minimum of two years' imprisonment and a fine of thirty million lire if the offense is particularly serious.

Anyone who, for profit, reproduces, transfers to another medium, distributes, communicates, presents, or demonstrates in public the contents of a database on media not marked pursuant

to this law in violation of the provisions of Articles 64 quinquies and 64 sexies, or extracts or reuses the database in violation of the provisions of Articles 102 bis and 102 ter, or distributes, sells, or leases a database, is subject to imprisonment from six months to three years and a fine of between five million and thirty million lire. The penalty is not less than two years' imprisonment and a fine of thirty million lire if the offense is particularly serious.

- ***Art. 171- ter (L.633/1941)***

Anyone who commits the act for profit for non-personal use will be punished with imprisonment from six months to three years and a fine from five to thirty million lire:

a) unlawfully duplicates, reproduces, transmits or publicly disseminates, in whole or in part, by any means, an intellectual work intended for television, cinema, retail or rental, discs, tapes or similar media or any other media containing phonograms or videograms of musical, cinematographic or similar audiovisual works or sequences of moving images;

b) unlawfully reproduces, transmits or publicly disseminates, by any means, works or parts of literary, dramatic, scientific or educational, musical or dramatic-musical, or multimedia works, even if included in collective or composite works or databases;

c) even if he has not participated in the duplication or reproduction, introduces into the territory of the State, holds for sale or distribution, distributes, places on the market, rents out or otherwise transfers for any reason, shows in public, broadcasts by television using any method, broadcasts by radio, makes public listening to the illegal duplications or reproductions referred to in letters a) and b);

d) holds for sale or distribution, places on the market, sells, rents, transfers under any title, projects in public, broadcasts by radio or television by any means, video cassettes, music cassettes, any medium containing phonograms or videograms of musical, cinematographic or audiovisual works or sequences of moving images, or other medium for which the affixing of a mark is prescribed pursuant to this law, without the mark itself or bearing a counterfeit or altered mark(2);

e) in the absence of an agreement with the legitimate distributor, retransmits or disseminates by any means an encrypted service received by means of equipment or parts of equipment suitable for decoding conditional access transmissions;

f) introduces into the territory of the State, possesses for sale or distribution, distributes, sells, rents, assigns for any reason, commercially promotes, installs special decoding devices or elements that allow access to an encrypted service without paying the fee due;

f-bis) manufactures, imports, distributes, sells, rents, assigns for any reason, advertises for sale or rental, or holds for commercial purposes, equipment, products, or components, or provides services that have the primary purpose or commercial use of circumventing effective technological measures referred to in Article 102-quater, or are primarily designed, produced, adapted, or created with the purpose of enabling or facilitating the circumvention of such measures. Technological measures include those

applied, or which remain, following the removal of such measures as a result of voluntary initiative by the rights holders or agreements between the latter and the beneficiaries of exceptions, or following the enforcement of administrative or judicial authority orders;

h) unlawfully removes or alters the electronic information referred to in Article 102 quinquies, or distributes, imports for distribution purposes, broadcasts by radio or television, communicates or makes available to the public works or other protected materials from which the electronic information itself has been removed or altered.

h-bis) abusively, even with the methods indicated in paragraph 1 of the article 85 of the consolidated text of the public safety laws, pursuant to Royal Decree 18 June 1931, no. 773, carries out the fixation on digital, audio, video or audio-video media, in whole or in part, of a cinematographic, audiovisual or editorial work or carries out the reproduction, performance or communication to the public of the illegally performed fixation(1).

Anyone who: is punished with imprisonment from one to four years and a fine from five to thirty million lire:

a) reproduces, duplicates, transmits or distributes illegally, sells or otherwise places on the market, transfers for any reason or illegally imports more than fifty copies or specimens of works protected by copyright and related rights;

a-bis) in violation of Article16, for profit, communicates to the public by placing it in a telematic network system, through connections of any kind, a work of the mind protected by copyright, or part of it;

b) by carrying out, in an entrepreneurial manner, the activities of reproduction, distribution, sale or marketing, or importation of works protected by copyright and related rights, is guilty of the acts set forth in paragraph 1;

c) promotes or organizes the illicit activities referred to in paragraph 1.

The penalty is reduced if the act is particularly trivial.

Conviction for one of the crimes set out in paragraph 1 entails:

a) the application of the accessory penalties referred to in the articles 30 and 32 of the penal code;

b) the publication of the judgment pursuant to Article 36 of the penal code;

c) the suspension for a period of one year of the concession or authorization for radio and television broadcasting for the exercise of the production or commercial activity.

The amounts resulting from the application of the pecuniary sanctions provided for in the previous paragraphs shall be paid to the National Social Security and Welfare Institute for Painters and Sculptors, Musicians, Writers and Playwrights.

- ***Art. 171-septies (L.633/1941)***

The penalty referred to in Article 171 ter, paragraph 1, also applies to:

a) [to producers or importers of media not subject to the marking referred to in Article 181 bis, who do not communicate to SIAE within thirty days from the date of placing on the market in the national territory or of importation the data necessary for the unequivocal identification of the media themselves;]

b) unless the act constitutes a more serious crime, to anyone who falsely declares that the obligations referred to in Article 181 bis, paragraph 2, of this law have been fulfilled.

- ***Art. 171 -octies (L.633/1941)***

Unless the act constitutes a more serious crime, anyone who fraudulently manufactures, sells, imports, promotes, installs, modifies, or uses for public or private purposes equipment or parts of equipment for decoding audiovisual broadcasts with conditional access broadcast over the airwaves, via satellite, or via cable, whether analog or digital, is punishable by imprisonment from six months to three years and a fine from €2,582 to €25,822. Conditional access is defined as all audiovisual signals transmitted by Italian or foreign broadcasters in such a way as to make them visible exclusively to closed groups of users selected by the broadcaster, regardless of the imposition of a fee for the use of this service.

The penalty is not less than two years of imprisonment and a fine of €15,493.00 if the offense is of significant seriousness.

14. Crime of Inducement to Refuse to Make Statements or to Make False Statements to the Judicial Authority (Article 25-decies of Legislative Decree 231/01)

Law 3 August 2009, n. 116 introduced the crime of "***Inducement to not make statements or to make false statements to the judicial authority***" all'art. 25- *ten times*of D.Lgs. 231/01.

This criminal hypothesis - already contemplated by Legislative Decree 231/01 among the transactional crimes (art. 10, paragraph 9, Law 146/2006) - now assumes relevance also at a national level.

Article 25 million

Inducement to not make statements or to make false statements to the judicial authority

!. In relation to the commission of the crime referred to in Article 377-bis of the Civil Code, the entity is subject to a pecuniary sanction of up to five hundred shares.

- ***Inducement to withhold or make false statements to the Judicial Authority (Article 377-bis of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who, by violence or threats, or by the offer or promise of money or other benefits, induces a person called upon to make statements

before a judicial authority that may be used in criminal proceedings, when the person has the right to remain silent, not to make a statement or to make false statements, shall be punished with imprisonment from two to six years.

15. The types of environmental offenses (Art. 25-Eleven of Legislative Decree No. 231/01)

Legislative Decree no. 121 of 7 July 2011, which implements Directive 2008/99/EC and Directive 2009/123/EC, following the obligation imposed by the European Union to criminalize behaviors that are highly dangerous for the environment, introduced art. 25*eleven times*of D.Lgs. 231/01.

Art. 25-undecies

Environmental crimes

1. In relation to the commission of the crimes provided for by the Criminal Code, the following pecuniary sanctions apply to the entity:

a) for the violation of Article 452-bis, a pecuniary sanction of between two hundred and fifty and six hundred quotas;

b) for violation of Article 452-quater, a pecuniary sanction of between four hundred and eight hundred shares;

c) for violation of Article 452-quinquies, a pecuniary sanction of between two hundred and five hundred shares;

d) for aggravated associative crimes pursuant to Article 452-octies, a pecuniary sanction ranging from three hundred to one thousand shares;

e) for the crime of trafficking and abandonment of highly radioactive material pursuant to Article 452-sexies, a pecuniary sanction of between two hundred and fifty and six hundred quotas;

f) for violation of Article 727-bis, a pecuniary sanction of up to two hundred and fifty quotas;

g) for violation of Article 733-bis, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas.

1-bis. In cases of conviction for the crimes indicated in paragraph 1, letters a) and b), of this Article, in addition to the pecuniary sanctions provided therein, the disqualification sanctions provided for in Article 9 shall apply, for a period not exceeding one year for the crime referred to in the aforementioned letter a).

2. In relation to the commission of the crimes provided for by Legislative Decree no. 152 of 3 April 2006, the following pecuniary sanctions shall apply to the entity:

a) for the crimes referred to in Article 137:

1) for the violation of paragraphs 3, 5, first period, and 13, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

2) for violation of paragraphs 2, 5, second period, and 11, a pecuniary sanction of between two hundred and three hundred quotas.

b) for the crimes referred to in Article 256:

1) for the violation of paragraphs 1, letter a), and 6, first period, a pecuniary sanction of up to two hundred and fifty quotas;

2) for the violation of paragraphs 1, letter b), 3, first period, and 5, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

3) for violation of paragraph 3, second period, a pecuniary sanction of between two hundred and three hundred quotas;

c) for the crimes referred to in Article 257:

1) for violation of paragraph 1, a pecuniary sanction of up to two hundred and fifty quotas;

2) for the violation of paragraph 2, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

d) for violation of Article 258, paragraph 4, second sentence, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

e) for violation of Article 259, paragraph 1, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

f) for the crime referred to in Article 260, a pecuniary sanction of between three hundred and five hundred shares, in the case provided for in paragraph 1, and between four hundred and eight hundred shares in the case provided for in paragraph 2;

g) for the violation of Article 260-bis, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas in the case provided for in paragraphs 6, 7, second and third periods, and 8, first period, and a pecuniary sanction of between two hundred and three hundred quotas in the case provided for in paragraph 8, second period;

h) for violation of Article 279, paragraph 5, a pecuniary sanction of up to two hundred and fifty quotas.

3. In relation to the commission of the crimes provided for by Law No. 150 of 7 February 1992, the following pecuniary sanctions apply to the entity:

a) for the violation of Articles 1, paragraph 1, 2, paragraphs 1 and 2, and 6, paragraph 4, a pecuniary sanction of up to two hundred and fifty quotas;

b) for the violation of Article 1, paragraph 2, a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

c) for the criminal code crimes referred to in Article 3-bis, paragraph 1, of the same Law no. 150 of 1992, respectively:

1) a pecuniary sanction of up to two hundred and fifty quotas, in the case of the commission of crimes for which the maximum penalty is not exceeding one year of imprisonment;

2) a pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas, in the event of the commission of crimes for which the maximum penalty provided is not exceeding two years of imprisonment;

3) a pecuniary sanction of between two hundred and three hundred quotas, in the event of the commission of crimes for which the maximum penalty provided is no more than three years of imprisonment;

4) a pecuniary sanction of between three hundred and five hundred quotas, in the event of the commission of crimes for which a maximum penalty of more than three years of imprisonment is foreseen.

4. In relation to the commission of the crimes provided for in Article 3, paragraph 6, of Law No. 549 of 28 December 1993, the entity shall be subject to a pecuniary sanction ranging from one hundred and fifty to two hundred and fifty quotas.

5. In relation to the commission of the crimes provided for by Legislative Decree no. 202 of 6 November 2007, the following pecuniary sanctions apply to the entity:

a) for the crime referred to in Article 9, paragraph 1, a pecuniary sanction of up to two hundred and fifty quotas;

b) for the crimes referred to in Articles 8, paragraph 1, and 9, paragraph 2, the pecuniary sanction of between one hundred and fifty and two hundred and fifty quotas;

c) for the crime referred to in Article 8, paragraph 2, a pecuniary sanction of between two hundred and three hundred quotas.

6. The sanctions provided for in paragraph 2, letter b), are reduced by half in the case of commission of the crime provided for in Article 256, paragraph 4, of Legislative Decree no. 152 of 3 April 2006.

7. In cases of conviction for the crimes indicated in paragraph 2, letters a), n. 2), b), n. 3), and f), and in paragraph 5, letters b) and c), the disqualification sanctions provided for in Article 9, paragraph 2, of Legislative Decree 8 June 2001, n. 231, shall apply for a period not exceeding six months.

8. If the entity or one of its organizational units is used on a permanent basis for the sole or primary purpose of enabling or facilitating the commission of the crimes referred to in Article 260 of Legislative Decree No. 152 of 3 April 2006 and Article 8 of Legislative Decree No. 202 of 6 November 2007, the sanction of permanent disqualification from exercising the activity shall apply pursuant to Article 16, paragraph 3, of Legislative Decree No. 231 of 8 June 2001.

The criminal offences referred to in Article 25*undecies* are as follows.

CRIMES INTRODUCED INTO THE PENAL CODE

- ***Environmental pollution (art. 452-bis.)***

Anyone who unlawfully causes significant and measurable impairment or deterioration shall be punished with imprisonment from two to six years and a fine from 10,000 to 100,000 euros:

1) of water or air, or of large or significant portions of the soil or subsoil;
2) of an ecosystem, of biodiversity, including agricultural biodiversity, of flora or fauna.
When pollution occurs in a protected natural area or one subject to landscape, environmental, historical, artistic, architectural, or archaeological restrictions, or to the detriment of protected animal or plant species, the penalty is increased from one-third to one-half. If pollution causes deterioration, impairment, or destruction of a habitat within a protected natural area or one subject to landscape, environmental, historical, artistic, architectural, or archaeological restrictions, the penalty is increased from one-third to two-thirds.

- ***Environmental disaster (art. 452-quater.)***

Except in the cases provided for in Article 434, anyone who unlawfully causes an environmental disaster is punishable by imprisonment from five to fifteen years.

The following alternatively constitute environmental disasters:

1) the irreversible alteration of the balance of an ecosystem;
2) the alteration of the balance of an ecosystem whose elimination is particularly costly and achievable only with exceptional measures;
3) the offense to public safety due to the relevance of the act to the extent of the compromise or its harmful effects or to the number of people offended or exposed to danger.

When the disaster occurs in a protected natural area or one subject to landscape, environmental, historical, artistic, architectural, or archaeological restrictions, or to the detriment of protected animal or plant species, the penalty is increased by one-third to one-half.

- ***Negligent crimes against the environment (Art. 452-quinquies.)***

If any of the acts referred to in Articles 452-bis and 452-quater are committed through negligence, the penalties provided for in those articles are reduced by one-third to two-thirds. If the commission of the acts referred to in the previous paragraph creates a risk of environmental pollution or environmental disaster, the penalties are further reduced by one-third.

- ***Trafficking and abandonment of highly radioactive material (Art. 452-sexies)***

Unless the act constitutes a more serious crime, anyone who unlawfully sells, purchases, receives, transports, imports, exports, procures for others, holds, transfers, abandons, or unlawfully disposes of highly radioactive material is punishable by imprisonment for two to six years and a fine of €10,000 to €50,000.

The penalty referred to in the first paragraph is increased if the act results in the risk of compromise or deterioration:

1) of water or air, or of large or significant portions of the soil or subsoil;
2) of an ecosystem, biodiversity, including agricultural biodiversity, flora, or fauna. If the act poses a threat to the life or safety of others, the penalty is increased by up to half.

- ***Aggravating circumstances (Art. 452-octies.)***

When the association referred to in Article 416 is directed, exclusively or concurrently, toward the purpose of committing one of the crimes provided for in this Title, the penalties provided for in Article 416 are increased. When the association referred to in Article 416-bis is aimed at committing one of the crimes provided for in this Title or at acquiring management or otherwise control of economic activities, concessions, authorizations, contracts, or public services relating to the environment, the penalties provided for in Article 416-bis are increased.

The penalties referred to in the first and second paragraphs are increased by one-third to one-half if the association includes public officials or persons in charge of a public service who exercise functions or perform services in environmental matters.

- ***Killing, destruction, capture, removal, or possession of specimens of protected wild animal or plant species (Article 727-bis of the Criminal Code)***

Unless the act constitutes a more serious crime, anyone who, outside of permitted circumstances, kills, captures, or possesses specimens belonging to a protected wild animal species is punishable by imprisonment for one to six months or a fine of up to €4,000, except when the action involves a negligible quantity of such specimens and has a negligible impact on the conservation status of the species. Anyone who, outside of permitted circumstances, destroys, takes, or possesses specimens belonging to a protected wild plant species is punishable by a fine of up to €4,000, except when the action involves a negligible quantity of such specimens and has a negligible impact on the conservation status of the species.

Unless the act constitutes a more serious crime, anyone who, outside of the permitted cases, violates the marketing prohibitions set out in theArticle 8, paragraph 2, of the Presidential Decree
September 8, 1997, No. 357, is punishable by imprisonment from two to eight months and a fine of up to 10,000 euros.

- ***Destruction or deterioration of habitats within a protected site (Article 733-bis of the Criminal Code)***

Anyone who, outside of permitted circumstances, destroys a habitat within a protected site or otherwise deteriorates it, compromising its state of conservation, is punishable by imprisonment of up to eighteen months and a fine of no less than €3,000.

CRIMES PROVIDED FOR BY THE "ENVIRONMENTAL CONCENTRATE"

- ***Criminal sanctions (art. 137– paragraphs 2,3,5,11,13 – Legislative Decree no. 152/2006, - T.U.***
  of the environment)

c. 2) Unauthorized discharge or discharge of hazardous substances.

When the conduct described in paragraph 1 concerns the discharge of industrial wastewater containing hazardous substances included in the families and groups of substances indicated

in Tables 5 and 3/A of Annex 5 to Part Three of this Decree, the penalty is imprisonment for a period of three months to three years and a fine of between €5,000 and €52,000.

c. 3) Discharge in violation of the regulations.

Anyone who, outside the cases referred to in paragraph 5 or in Article 29-quattuordecies, paragraph 3, discharges industrial wastewater containing the hazardous substances included in the families and groups of substances indicated in Tables 5 and 3/A of Annex 5 to Part Three of this Decree without complying with the requirements of the authorization, or the other requirements of the competent authority pursuant to Articles 107, paragraph 1, and 108, paragraph 4, shall be punished with imprisonment of up to two years.

c. 5) Discharge in violation of the table limits.

Unless the act constitutes a more serious crime, anyone who, in discharging industrial wastewater, exceeds the limit values set in Table 3 or, in the case of discharge to land, in Table 4 of Annex 5 to Part Three of this decree, or the more restrictive limits set by the regions or autonomous provinces or the competent authority pursuant to Article 107, paragraph 1, in relation to the substances listed in Table 5 of Annex 5 to Part Three of this decree, is punishable by imprisonment for up to two years and a fine of between €3,000 and €30,000. If the limit values set for the substances contained in Table 3/A of the same Annex 5 are also exceeded, imprisonment for between six months and three years and a fine of between €6,000 and €120,000 shall apply.

c. 11) Prohibition of discharge into subsoil and groundwater.

Anyone who fails to comply with the discharge prohibitions set forth in Articles 103 and 104 is punishable by imprisonment of up to three years.

c. 13) Discharge into the sea by ships or aircraft.

The penalty of imprisonment from two months to two years always applies if the discharge into the sea from ships or aircraft contains substances or materials whose discharge is absolutely prohibited pursuant to the provisions of the international conventions in force on the matter and ratified by Italy, unless they are in quantities such as to be rapidly rendered harmless by the physical, chemical, and biological processes that occur naturally at sea and provided that prior authorization from the competent authority is obtained.

- Unauthorized waste management activities (art. 256 – paragraphs 1a, 1b, 3 first and second periods, 4 5, 6 first period – Legislative Decree no. 152 / 2006 – Consolidated Law on the Environment)

c. 1 a, b) Waste management without authorization.

Anyone who carries out waste collection, transport, recovery, disposal, trade or intermediation activities without the required authorisation, registration or communication referred to in Articles 208, 209, 210, 211, 212, 214, 215 and 216 shall be punished:

a) with a penalty of imprisonment from three months to one year or a fine from 2,600 to 26,000 euros if the waste is non-hazardous;

b) with a penalty of imprisonment from six months to two years and a fine from 2,600 euros to 26,000 euros if the waste involves hazardous waste.

c. 3) Construction and management of an unauthorized landfill.

Anyone who builds or operates an unauthorized landfill is punishable by six months to two years of imprisonment and a fine ranging from €2,600 to €26,000. Imprisonment for one to three years and a fine ranging from €5,200 to €52,000 applies if the landfill is used, even in part, for the disposal of hazardous waste. A conviction or a sentence issued pursuant to Article 444 of the Code of Criminal Procedure shall result in the confiscation of the area on which an illegal landfill is built if it is owned by the perpetrator or an accomplice to the crime, without prejudice to the obligations to clean up or restore the site to its original condition.

c. 5) Prohibition of mixing waste.

Anyone who, in violation of the prohibition set forth in Article 187, carries out unauthorized waste mixing activities shall be punished with the penalty set forth in paragraph 1, letter b).

c. 6) Storage of medical waste.

Anyone who temporarily stores hazardous medical waste at the site of production, in violation of the provisions of Article 227, paragraph 1, letter b), is punishable by imprisonment for three months to one year or a fine ranging from €2,600 to €26,000. An administrative fine ranging from €2,600 to €15,500 applies for quantities not exceeding 200 liters or equivalent quantities.

- ***Site remediation (art. 257 – paragraphs 1, 2 – Legislative Decree no. 152 / 2006 – Consolidated Environmental Law) c. 1) Failure to remediate sites.***

Unless the act constitutes a more serious crime, anyone who causes pollution of the soil, subsoil, surface water, or groundwater by exceeding the risk threshold concentrations is punishable by imprisonment for six months to one year or a fine of €2,600 to €26,000 if they fail to carry out the remediation in accordance with the plan approved by the competent authority under the procedure referred to in Articles 242 et seq. Failure to provide the notification referred to in Article 242, the offender is punished by imprisonment for three months to one year or a fine of €1,000 to €26,000.

c. 2) Dangerous substances.

The penalty is imprisonment from one to two years and a fine from €5,200 to €52,000 if the pollution is caused by dangerous substances.

Compliance with the projects approved pursuant to Articles 242 et seq. constitutes a condition for non-punishability for environmental violations provided for by other laws for the same event and for the same pollution conduct referred to in paragraph 1.

- ***Violation of reporting obligations, mandatory register keeping and forms (Article 258 – paragraph 4, second sentence – Legislative Decree no. 152/2006 – Consolidated Law of the environment)***

c. 4) Transport of waste without a form.

The law punishes, with an administrative pecuniary sanction, anyone who transports waste without the identification form (FIR) referred to in Article 193 or without the substitute documents provided for therein, or anyone who reports incomplete or inaccurate data in the form itself.

The penalty set forth in Article 483 of the Criminal Code applies to anyone who transports hazardous waste, including anyone who, when preparing a waste analysis certificate, provides false information about the nature, composition, and chemical-physical characteristics of the waste, and anyone who uses a false certificate during transportation.

- ***Illicit waste trafficking (Article 259 – paragraph 1 – Legislative Decree no. 152 / 2006 – Consolidated Law on the Environment)***

c. 1) Transboundary shipment of waste, constituting illicit trafficking.

Anyone who ships waste that constitutes illicit trafficking pursuant to Article 26 of Regulation (EEC) No. 259 of 1 February 1993, or ships waste listed in Annex II of the aforementioned regulation in violation of Article 1, paragraph 3, letters a), b), c), and d), of the same regulation, is punishable by a fine ranging from €1,550 to €26,000 and imprisonment for up to two years. The penalty is increased for shipments of hazardous waste.

- ***Organized activities for the illicit trafficking of waste (Article 452-quaterdecies of the Criminal Code)***

c. 1) Illegal waste management.

Anyone who, for the purpose of obtaining an unjust profit, through multiple transactions and through the establishment of organized means and ongoing activities, sells, receives, transports, exports, imports, or otherwise illegally manages large quantities of waste is punishable by imprisonment for one to six years.

c. 2) Highly radioactive waste.

If the waste is highly radioactive, the penalty is three to eight years of imprisonment.

- ***Computerized waste traceability control system (Art. 260-bis – paragraphs 6, 7 second and third periods, 8 – Legislative Decree no. 152 / 2006 – Consolidated Law on the Environment)***

c. 6) False information in the waste traceability certificate.

The penalty set forth in Article 483 of the Criminal Code applies to anyone who, in preparing a waste analysis certificate used within the waste traceability control system, provides false information on the nature, composition, and chemical-physical characteristics of the waste, and to anyone who includes a false certificate among the data to be provided for waste traceability purposes.

c. 7) Transport of hazardous waste without a copy of the Sistri form or using a form with false information.

The penalty set forth in Article 483 of the Criminal Code applies to the transportation of hazardous waste. This penalty also applies to anyone who, during transportation, uses a

waste analysis certificate containing false information regarding the nature, composition, and chemical-physical characteristics of the transported waste.

c. 8) Transport of waste with a fraudulently altered Sistri card.

Any transporter who accompanies waste shipments with a fraudulently altered paper copy of the SISTRI - HANDLING AREA form is punishable by the penalty provided for in the combined provisions of Articles 477 and 482 of the Criminal Code. The penalty is increased by up to one-third in the case of hazardous waste.

- ***Sanctions (art. 279 – paragraph 5 – Legislative Decree no. 152 / 2006 – Consolidated Law on the Environment)***

c. 5) Exceeding emission limits and exceeding air quality limit values.

In the cases provided for in paragraph 2, the penalty of imprisonment of up to one year always applies if exceeding the emission limit values also results in exceeding the air quality limit values provided for by current legislation.

CRIMES RELATED TO THE PROTECTION OF ANIMAL AND PLANT SPECIES

- ***Art. 1 – paragraphs 1, 2 – Law no. 150/1992***

1. Unless the act constitutes a more serious crime, anyone who violates the provisions of Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments, for specimens belonging to the species listed in Annex A of the same Regulation and subsequent amendments, shall be punished with imprisonment for a period of six months to two years and a fine of between fifteen thousand and one hundred and fifty thousand euros:

a) imports, exports or re-exports specimens, under any customs regime, without the required certificate or licence, or with a certificate or licence which is not valid pursuant to

of Article 11, paragraph 2a of Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments;

b) fails to comply with the requirements aimed at the safety of the specimens, specified in a permit or certificate issued in accordance with Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments, and Commission Regulation (EC) No. 939/97 of 26 May 1997, and subsequent amendments;

c) uses the aforementioned specimens in a manner that is not in accordance with the provisions contained in the authorisation or certification provisions issued together with the import licence or certified subsequently;

d) transports or transits, even on behalf of third parties, specimens without the required permit or certificate, issued in accordance with Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments, and Commission Regulation (EC) No. 939/97 of 26 May 1997 and subsequent amendments and, in the case of export or re-export from a third country that is a party to the Washington Convention, issued in accordance with the same, or without sufficient proof of their existence;

e) trades in artificially propagated plants in breach of the provisions established pursuant to Article 7, paragraph 1, letter b), of Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments and of Regulation (EC) No. 939/97 of the Commission of 26 May 1997 and subsequent amendments;

f) holds, uses for profit, purchases, sells, displays or holds for sale or for commercial purposes, offers for sale or otherwise transfers specimens without the required documentation.

2. In the event of a repeat offense, the penalty is one to three years' imprisonment and a fine ranging from thirty thousand to three hundred thousand euros. If the aforementioned offense is committed in the course of a business activity, the conviction results in a license suspension of a minimum of six months and a maximum of two years;

- ***Art. 2 – paragraphs 1, 2 – Law no. 150/1992***

1. Unless the act constitutes a more serious crime, anyone who, in violation of the provisions of Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments, for specimens belonging to the species listed in Annexes B and C of the same Regulation, shall be punished with a fine of between twenty thousand and two hundred thousand euros or with imprisonment of between six months and one year:

a) imports, exports or re-exports specimens, under any customs regime, without the required certificate or licence, or with a certificate or licence that is not valid pursuant to Article 11, paragraph 2a of Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments;

b) fails to comply with the requirements aimed at the safety of the specimens, specified in a permit or certificate issued in accordance with Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments and Regulation (EC) No. 939/97
from the Commission of the 26 May 1997 and successive modifications;

c) uses the aforementioned specimens in a manner that is not in accordance with the provisions contained in the authorisation or certification provisions issued together with the import licence or certified subsequently;

d) transports or transits, even on behalf of third parties, specimens without the required licence or certificate, issued in accordance with Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments, and Commission Regulation (EC) No. 939/97 of 26 May 1997 and subsequent amendments and, in the case of export or re-export from a third country that is a party to the Washington Convention, issued in accordance with the same, or without sufficient proof of their existence;

e) trades in artificially propagated plants in breach of the provisions established pursuant to Article 7, paragraph 1, letter b), of Council Regulation (EC) 338/97 of 9 December 1996, and subsequent implementations and amendments and of Regulation (EC) No. 939/97 of the Commission of 26 May 1997 and subsequent amendments;

f) holds, uses for profit, purchases, sells, exhibits or holds for sale or for commercial purposes, offers for sale or otherwise transfers specimens without the required documentation, limited to the species listed in Annex B of the Regulation.

2. In the event of a repeat offense, the penalty is imprisonment from six to eighteen months and a fine from twenty thousand to two hundred thousand euros. If the aforementioned offense is committed in the exercise of business activities, the conviction results in license suspension from a minimum of six months to a maximum of eighteen months.

- ***Art. 3 bis – paragraph 1 – Law no. 150/1992***

1. The offences referred to in Article 16, paragraph 1, letters a), c), d), e), and l), of Council Regulation (EC) No. 338/97 of 9 December 1996, and subsequent amendments, concerning the falsification or alteration of certificates, licences, import notifications, declarations, and communications of information for the purpose of acquiring a licence or certificate, and the use of false or altered certificates or licences, shall be subject to the penalties set out in Book II, Title VII, Chapter III of the Criminal Code.

- ***Art. 6 – paragraph 4 – Law no. 150/1992***

4. Anyone who violates the provisions of paragraph 1 shall be punished with imprisonment of up to six months or with a fine of between fifteen thousand and three hundred thousand euros.

CRIMES CONNECTED AT THE PROTECTION OF THE LAYER FROM OZONE AND THE ENVIRONMENT

- ***Cessation and reduction of the use of harmful substances (Article 3 – paragraph 6 – Law no. 549/1993)***

6. Anyone who violates the provisions of this article is punishable by imprisonment for up to two years and a fine of up to three times the value of the substances used for production, import, or trade. In the most serious cases, the conviction results in the revocation of the authorization or license under which the illegal activity was conducted.

CRIMES RELATED TO POLLUTION CAUSED BY SHIPS

- ***Intentional pollution (art. 8 of Legislative Decree no. 202/2007)***

1. Unless the act constitutes a more serious crime, the Master of a vessel, flying any flag, as well as the crew members, the owner, and the vessel's operator, if the violation occurred with their complicity, who willfully violate the provisions of Article 4 shall be punished by imprisonment for six months to two years and a fine of €10,000 to €50,000.

2. If the violation referred to in paragraph 1 causes permanent or, in any case, particularly serious damage to the quality of water, to animal or plant species, or to parts thereof, the penalty is imprisonment for one to three years and a fine of between €10,000 and €80,000.

3. Damage is considered particularly serious when eliminating its consequences is particularly complex from a technical perspective, or particularly onerous or achievable only with exceptional measures.

- ***Negligent pollution (art. 9 of Legislative Decree no. 202/2007)***

1. Unless the act constitutes a more serious crime, the Master of a vessel, flying any flag, as well as the crew members, the owner, and the vessel's operator, if the violation occurred with their complicity, who willfully violate the provisions of Article 4 shall be punished by imprisonment for six months to two years and a fine of €10,000 to €30,000.

2. If the violation referred to in paragraph 1 causes permanent or, in any case, particularly serious damage to the quality of water, to animal or plant species, or to parts thereof, the penalty is imprisonment for 6 months to two years and a fine of between €10,000 and €30,000.

3. Damage is considered particularly serious when eliminating its consequences is particularly complex from a technical perspective, or particularly onerous or achievable only with exceptional measures.

- ***Sanctions against the Entity pursuant to Legislative Decree no. 121/2011***

A pecuniary penalty is applicable to all situations for which the entity is held liable. The delegated legislator has established three categories of severity, as detailed below:

- pecuniary penalty of 150 to 250 quotas for crimes punishable by imprisonment of up to two years or by arrest of up to two years;
- pecuniary sanction of up to 250 quotas for crimes punishable by a fine or by a prison sentence of up to one year or a prison sentence of up to two years (combined with the fine);
- pecuniary penalty of 200 to 300 quotas for crimes punishable by imprisonment of up to three years or by arrest of up to three years.

This scheme is an exception to the crime referred to in art. 260, paragraph 1 of Law 152/06 (Consolidated Law on the Environment), for which the most severe sanctioning regime is reserved, as described below, for activities organized for the illicit trafficking of waste:

- pecuniary sanctions from 300 to 500 quotas.

The application of prohibitive sanctions – pursuant to art. 9 paragraph 2 of Legislative Decree 231/01 – against legal entities is envisaged exclusively in the following cases:

1) art. 137, paragraphs 2, 5 second period, and 11 of Legislative Decree no. 152/2006;

2) art. 256, paragraph 3 - second sentence - Legislative Decree no. 152/2006; 3) art. 260 paragraphs 1 and 2 of Legislative Decree no. 152/2006.

Only in these cases, therefore, will it be possible to apply the same precautionary sanctions to the legal entity pursuant to Articles 45 et seq. of Legislative Decree no. 231/01.

The application of the most serious sanction among those provided for by Legislative Decree no. 231/01, namely that of permanent disqualification from carrying out the activity referred to in art. 16, paragraph 3, was established in cases where the legal person or one of its organizational activities is permanently used for the sole or prevalent purpose of enabling or facilitating the commission of the crimes of conspiracy for the purpose of illicit waste trafficking (art. 260, Legislative Decree no. 152/2006, paragraphs 1 and 2).

16. Crime of employment of third-country nationals whose stay is irregular (Article 25-duodecies of Legislative Decree no. 231/01)

Legislative Decree 16 July 2012, n. 109, art.2, introduced the crime of "***Employment of foreign citizens whose stay is irregular"***all'art. 25-*twelve times*of Legislative Decree 231/01, which provides for the application of a pecuniary sanction to the entity for this crime of 100 to 200 quotas, up to a limit of 150,000 euros.

Article 25-twelve.

Employment of third-country nationals whose stay is irregular

1. In relation to the commission of the crime referred to in Article 22, paragraph 12-bis, of Legislative Decree no. 286 of 25 July 1998, a pecuniary sanction of 100 to 200 quotas, up to a limit of 150,000 euros, shall apply to the entity.

1-bis. In relation to the commission of the crimes referred to in Article 12, paragraphs 3, 3-bis, and 3-ter, of the consolidated text of Legislative Decree No. 286 of 25 July 1998, and subsequent amendments, the entity shall be subject to a pecuniary sanction ranging from four hundred to one thousand quotas.

1-ter. In relation to the commission of the crimes referred to in Article 12, paragraph 5, of the consolidated text of Legislative Decree No. 286 of 25 July 1998, and subsequent amendments, the entity shall be subject to a pecuniary sanction of between one hundred and two hundred quotas.

1-quater. In cases of conviction for the crimes referred to in paragraphs 1-bis and 1-ter of this article, the disqualification sanctions provided for in Article 9, paragraph 2, shall apply for a period of no less than one year.

The following criminal offense ("Employment of citizens of foreign countries whose stay is irregular") is governed by art. 22, paragraph 12-bis, of Legislative Decree no. 286 of 25 July 1998, as amended by Legislative Decree no. 145/2024, converted with amendments by Law no. 187/2024 (Consolidated text of provisions concerning immigration regulations and rules on the status of foreigners).

- ***"Employment of citizens of foreign countries whose stay is irregular***

The penalties for the act provided for in paragraph 12 of art. 22 of Legislative Decree no. 286 of 25 July 1998 - according to which:

"*The employer who employs foreign workers without the residence permit provided for in this article, or whose permit has expired and whose renewal has not been requested within the legal timeframe, or has been revoked or cancelled, shall be punished with imprisonment from six months to three years and a fine of 5,000 euros for each worker employed.*" - have increased by a third to a half:

a)if the number of employed workers is more than three;

b) if the employed workers are minors of non-working age;

c) if the employed workers are subjected to the other working conditions referred to in the third paragraph of Article 603-*until*of the penal code. "

Law 17 October 2017, n. 161, art.30, paragraph 4 introduced in art. 25-*twelve times*of the D.Lgs.
231/01 the crimes referred to in art. 12, paragraph 3, 3 bis, 3 ter and paragraph 5, Legislative Decree no. 286/1998
("**Provisions against illegal immigration"**) which provide for the application of a pecuniary sanction of between 400 and 1000 quotas to the entity for such crimes.

Legislative Decree no. 20/2023, converted with amendments by Law no. 50/2023, amended Article 12, paragraph 3, increasing the prison sentence from six to sixteen years.

- Transport of foreigners within the territory of the State (art. 12, paragraphs 3, 3 bis and 3 ter, Legislative Decree 25 July 1998 n. 286)

3. Unless the act constitutes a more serious crime, anyone who, in violation of the provisions of this Consolidated Law, promotes, directs, organizes, finances, or carries out the transportation of foreigners into the territory of the State or performs other acts aimed at illegally procuring their entry into the territory of the State, or of another State of which the person is not a citizen or does not have a permanent residence permit, shall be punished with imprisonment for six to sixteen years and a fine of €15,000 for each person if: a) the act concerns the illegal entry or stay in the territory of the State of five or more persons; b) the transported person has been exposed to danger to his or her life or safety in order to procure his or her illegal entry or stay; c) the transported person has been subjected to inhuman or degrading treatment in order to procure his or her illegal entry or stay; d) the act is committed by three or more persons in collusion with each other or using international transport services or forged, altered, or otherwise illegally obtained documents; e) the authors of the act have the**availability**of weapons or explosive materials.

3-bis. If the acts referred to in paragraph 3 are committed under two or more of the conditions referred to in letters a), b), c), d), and e) of the same paragraph, the penalty provided therein is increased.

3-ter. The prison sentence is increased from one-third to one-half and a fine of €25,000 applies to each person if the acts referred to in paragraphs 1 and 3: a) are committed for the purpose of recruiting persons for prostitution or sexual or labor exploitation, or involve the recruitment of minors to be employed in illicit activities in order to facilitate their exploitation; b) are committed for the purpose of profit, even indirectly.

- facilitating the permanence of foreigners in the territory of the state (art. 12, paragraph 5, Legislative Decree 25 July 1998 n. 286)

5. Outside the cases provided for in the preceding paragraphs, and unless the act constitutes a more serious crime, anyone who, with the aim of unfairly profiting from the illegal status of a foreigner or in the context of activities punishable under this article, facilitates the presence of that foreigner in the territory of the State in violation of the provisions of this Consolidated Law, is punishable by imprisonment of up to four years and a fine of up to thirty million lire. When the act is committed in concert by two or more persons, or involves the presence of five or more persons, the penalty is increased by one-third to one-half.

17. Crimes of racism and xenophobia (art. 25-*terdecies* of D.Lgs. n. 231/01)

Law 20 November 2017, n. 167, art. 2 introduced the crimes of racism and xenophobia to art. 25-*terdecies* of Legislative Decree 231/01 which provides for the application of a pecuniary sanction of 200 to 800 quotas to the entity for such crimes.

Art. 25-terdecies
Racism and xenophobia

((1. In relation to the commission of the crimes referred to in Article 3, paragraph 3-bis, of Law No. 654 of 13 October 1975, a pecuniary sanction of between two hundred and eight hundred shares shall apply to the entity.
2. In cases of conviction for the crimes referred to in paragraph 1, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity for a period of no less than one year.
3. If the entity or one of its organizational units is permanently used for the sole or prevalent purpose of allowing or facilitating the commission of the crimes indicated in paragraph 1, the sanction shall apply
of the definitive ban from carrying out the activity pursuant to Article 16, paragraph 3).

These criminal offences are governed by Article 3, paragraph 3-bis of Law 654/1975 (International Convention on the Elimination of All Forms of Racial Discrimination):

A prison sentence of two to six years applies if the propaganda or incitement, committed in such a way as to create a concrete risk of dissemination, is based in whole or in part on the denial, serious minimization, or apology of the Holocaust or the crimes of genocide, crimes against humanity, and war crimes, as defined in Articles 6, 7, and 8 of the Statute of the International Criminal Court, ratified pursuant to Law No. 232 of 12 July 1999.

18. Fraud in sports competitions, illegal gambling or betting, and gambling conducted using prohibited devices (Article 25-quaterdecies of Legislative Decree 231/01)

Law no. 39 of 30 May 2019 introduced Article 25-quaterdecies of Legislative Decree 231/01 into law, introducing fraud in sports competitions (Article 1 of Law 40/1989) and the crime of unauthorized gambling or betting (Article 4 of Law 401/1989).

Art. 25-quaterdecies

Fraud in sports competitions, illegal gambling or betting and gambling carried out using prohibited devices

1. In relation to the commission of the crimes referred to in Articles 1 and 4 of Law No. 401 of 13 December 1989, the following pecuniary sanctions shall apply to the entity:

a) for crimes, a pecuniary sanction of up to five hundred quotas;

b) for contraventions, a pecuniary sanction of up to two hundred and sixty quotas.

2. In cases of conviction for one of the crimes indicated in paragraph 1, letter a), of this article, the interdictory sanctions provided for in article 9, paragraph 2, shall apply for a period of no less than one year.

19. Tax crimes (art. 25-*quinquiesdecies* D.Lgs. 231/01)

Legislative Decree no. 124 of 26 October 2019 introduced tax crimes in art. 25-*quinquiesdecies,*comma 1, of Legislative Decree 231/2001. Depending on the type of crime, the entity is subject to a fine of 400 to 500 shares.

Subsequently, through the Legislative Decree of 5 November 2024 n. 173 (listed*"Consolidated Law on Administrative and Criminal Tax Penalties"*), the legislator intervened in the tax legislation of a sanctioning nature, carrying out a compilation intervention to relocate the administrative and criminal provisions: with the aforementioned decree, in fact, the administrative and criminal sanctioning provisions already in force were merged into a single law, maintaining their contents unchanged; the previous Legislative Decree no. 74/2000, consequently, was repealed but, as provided for by art. 102 of Legislative Decree no. 173/2024, the effective date of the new legislation is postponed to January 1, 2026.

Article 25-quinquiesdecies
Tax crimes

1. In relation to the commission of the crimes provided for by Legislative Decree no. 74 of 10 March 2000, the following pecuniary sanctions shall apply to the entity:
a) for the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions provided for in Article 2, paragraph 1, a pecuniary sanction of up to five hundred quotas;
b) for the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions, provided for in Article 2, paragraph 2-bis, a pecuniary sanction of up to four hundred quotas;
c) for the crime of fraudulent declaration through other artifices, as provided for in Article 3, a pecuniary sanction of up to five hundred quotas;

d) for the crime of issuing invoices or other documents for non-existent transactions, as provided for in Article 8, paragraph 1, a pecuniary sanction of up to five hundred quotas;
e) for the crime of issuing invoices or other documents for non-existent transactions, as provided for in Article 8, paragraph 2-bis, a pecuniary sanction of up to four hundred quotas;
f) for the crime of concealment or destruction of accounting documents, as provided for in Article 10, a pecuniary sanction of up to four hundred quotas;
g) for the crime of fraudulent evasion of tax payment, as provided for in Article 11, a pecuniary sanction of up to four hundred quotas.
((1-bis. In relation to the commission of the crimes provided for by Legislative Decree No. 74 of 10 March 2000, when they are committed for the purpose of evading VAT within the context of cross-border fraudulent schemes connected to the territory of at least one other Member State of the European Union, from which a total damage of ten million euros or more results or may result, the following pecuniary sanctions shall apply to the entity:
a) for the crime of false declaration provided for in Article 4, a pecuniary sanction of up to three hundred quotas;
b) for the crime of failure to declare as provided for in Article 5, a pecuniary sanction of up to four hundred quotas;
c) for the crime of undue compensation provided for in Article 10-quater, a pecuniary sanction of up to four hundred shares.
2. If, following the commission of the crimes indicated ((in paragraphs 1 and 1-bis)), the entity has obtained a significant profit, the pecuniary sanction is increased by one third.
3. In the cases provided for in ((paragraphs 1, 1-bis and 2)), the prohibitive sanctions referred to in Article 9, paragraph 2, letters c), d) and e) shall apply.

- ***Fraudulent declaration through the use of invoices or other documents for non-existent transactions (Article 2, paragraph 1 and 2-bis of Legislative Decree No. 74/2000;*****from 01/01/2026 new art. 74 Legislative Decree no. 173/2024*****)***

The law punishes with imprisonment from four to eight years anyone who, in order to evade income or value added taxes by using invoices or other documents for non-existent transactions, indicates fictitious liabilities in one of the declarations relating to such taxes.

If the amount of fictitious liabilities is less one hundred thousand euros, imprisonment from one year and six months applies six years.

- ***Fraudulent declaration through other artifices (art. 3 of Legislative Decree 74/2000;*****from 01/01/2026 new art. 75 Legislative Decree no. 173/2024*****)***

The law punishes with imprisonment from three to eight years anyone who, outside the cases provided for in Article 2, for the purpose of evading income or value added taxes, by carrying out objectively or subjectively simulated transactions or by using false documents or other fraudulent means capable of hindering the assessment and misleading the tax authorities, indicates in one of the declarations relating to said taxes assets for an amount lower than the actual amount or fictitious liabilities or fictitious credits and withholdings, when, jointly:

a) the evaded tax is higher, with reference to some of the individual taxes, than thirty thousand euros;
b) the total amount of assets subtracted from taxation, including through the indication of fictitious liabilities, is greater than five percent of the total amount of assets indicated in the declaration, or in any case, is greater than one million five hundred thousand euros, or if the total amount of fictitious credits and withholdings reducing the tax is greater than five percent of the amount of the tax itself or in any case thirty thousand euros.

The act is considered to have been committed using false documents when such documents are recorded in the mandatory accounting records or are held as evidence against the tax authorities.
It should be noted that the mere violation of the obligations to invoice and record assets in the accounting records or the mere indication in invoices or records of assets lower than the actual ones do not constitute fraudulent means.

- ***Issuing invoices for non-existent transactions (Article 8, paragraphs 1 and 2-bis, of Legislative Decree 74/2000;*****from 01/01/2026 new art. 79 Legislative Decree no. 173/2024*****)**

The law punishes with imprisonment from four to eight years anyone who, in order to enable third parties to evade income or value added taxes, issues or releases invoices or other documents for non-existent transactions.

If the amount indicated on the invoices or documents is less than one hundred thousand euros per tax period, imprisonment from one year and six months to six years applies.

- ***Concealment or destruction of accounting documents (art. 10 of Legislative Decree 74/2000;*****from 01/01/2026 new art. 81 Legislative Decree no. 173/2024*****)**

Unless the act constitutes a more serious crime, the law punishes with imprisonment from three to seven years anyone who, with the aim of evading income or value added taxes, or of enabling third parties to do so, conceals or destroys, in whole or in part, accounting records or documents required to be retained, in such a way as to prevent the reconstruction of income or turnover.

- ***Fraudulent evasion of tax payment (Article 11 of Legislative Decree 74/2000);*** **from 01/01/2026 new art. 85 Legislative Decree no. 173/2024*****)**

The law punishes with imprisonment from six months to four years anyone who, in order to evade payment of income or value added taxes or interest or administrative penalties relating to such taxes for a total amount exceeding fifty thousand euros, simulates the sale or carries out other fraudulent acts on their own or others' assets capable of rendering the forced collection procedure ineffective in whole or in part.

Article 25-quinquiesdecies was subsequently amended by the entry into force of Legislative Decree no. 75/2020, implementing Directive (EU) 2017/1371 on the protection of the financial

interests of the European Union (so-called PIF Directive), which inserted into the body of Article 25-*quinquiesdecies, in paragraph 1-bis the following crimes:*

- ***False declaration (art. 4 of Legislative Decree 74/2000;*****from 01/01/2026 new art. 76 Legislative Decree no. 173/2024*****)***
- ***Failure to declare (art. 5 of Legislative Decree 74/2000;*****from 01/01/2026 new art. 77 Legislative Decree no. 173/2024*****)***
- ***Undue compensation (art. 10-quater of Legislative Decree 74/2000;*****from 01/01/2026 new art. 84 Legislative Decree no. 173/2024*****)***

Paragraph 1-bis of Article 25-quinquiesdecies of Legislative Decree 231/01 provides for the application of the following pecuniary sanctions to the entity:
a) for the crime of false declaration, a pecuniary sanction of up to three hundred quotas;
b) for the crime of failure to declare, a pecuniary sanction of up to four hundred quotas;
c) for the crime of undue compensation, a pecuniary sanction of up to four hundred quote.

These tax crimes constitute predicate offences for the administrative liability of entities for crime only if:

- committed in the context of cross-border fraudulent schemes connected to the territory of at least one other Member State of the European Union;
- are aimed at evading VAT for an amount not less than 10 million euros.

Therefore, any violations that, although criminally relevant for natural persons (the crimes referred to, in fact, have much lower thresholds), do not exceed the specific punishability thresholds established for administrative offenses are not relevant for the purposes of corporate liability.

Having said this, the crime **of false declaration punishes** with imprisonment from two to four years the taxpayer who submits a false declaration, indicating assets for an amount lower than the actual amount or non-existent liabilities.

The conduct is further characterized by the lack of any elements of fraud, as also clarified by the proviso to the crimes of "tax fraud" pursuant to Articles 2 and 3 of Legislative Decree 74/2000. In particular, an incorrect declaration does not occur in the following cases: (i) incorrect classification of items accurately reported in the declaration; (ii) incorrect valuation of assets or liabilities, when the criteria actually applied were indicated in the financial statements or other relevant tax documentation; (iii) violation of the criteria for determining the accrual period; (iv) violation of the provisions regarding the relevance and deductibility of actual liabilities. Furthermore, valuations that, considered overall, differ less than 10 percent from the correct ones do not give rise to punishable acts. In short, Article Article 4 of Legislative Decree 74/2000 attributes criminal relevance only to liabilities that are materially non-existent, thus excluding all costs actually incurred. Furthermore, this reaffirms the criminal irrelevance of tax evasion, already established by Article 10, paragraph 13 of Legislative Decree 128/2015.

The **case of failure to declare**The Italian Criminal Code punishes with imprisonment from two to five years the conduct of anyone who, for the purpose of evading income taxes or VAT, fails to file a declaration relating to such taxes when required to do so. This offense is committed only after 90 days have elapsed following the deadline for filing the declaration. To accurately interpret this offense, it is necessary to consider the provisions of the tax law that identify the circumstances that make it mandatory for a taxpayer (Italian or foreign) to file a tax return. As stated above, this provision constitutes a predicate offense only in relation to the failure to file a VAT declaration.

Lastly, the**crime of undue compensation**Anyone who fails to pay taxes due by offsetting non-payable credits (i.e., credits whose existence and amount are certain, but are not yet or no longer usable for tax purposes) or non-existent credits (i.e., credits that have no basis in the taxpayer's tax position) is punishable by six months to two years of imprisonment. The offsetting of tax debts and credits can be "horizontal"—that is, between credits and debts of different nature—or "vertical," that is, between tax credits and debts of the same type. Legislative Decree no. 87/2024 amends this crime by providing for an exclusion from punishment in cases where, due to the technical nature of the assessments, there are objectively uncertain conditions regarding the specific elements or particular characteristics that establish the entitlement of the credit.

If, following the commission of the crimes indicated in paragraphs 1 and 1-bis, the entity has obtained a significant profit, the pecuniary sanction is increased by one third.

In relation to all the crimes provided for by art. 25-*quinquiesdecies* of Legislative Decree 231/01, the interdictory sanctions referred to in Article 9, paragraph 2, letters c), d) and e) apply.

20. Smuggling crimes (art. 25-*sexiesdecies*of the Decree)

Legislative Decree 75/2020, through the introduction of art. 25-*sexiesdecies*within Legislative Decree no. 231/01, the criminal offences of smuggling, provided for by Presidential Decree no. 43/1973 (the so-called “Consolidated Customs Act” or TULD), have been inserted as new crimes giving rise to the liability of the entity.

On 4 October 2024, Legislative Decree no. 141 of 26 September 2024, containing “*National provisions supplementing the Union Customs Code and reviewing the system of sanctions for excise duties and other indirect taxes on production and consumption.*through which the customs regulations and the sanctions system relating to customs, excise duties, and other indirect taxes on production and consumption were reorganized, with the aim of aligning Italian customs legislation with the Community legislation contained in EU Regulation 952/2013.

The new law, in addition to inserting into art. 25*sexiesdecies* of Legislative Decree 231/2001 the crimes provided for by Legislative Decree 504/1995 (Consolidated Law on Excise Duties), outlines new customs violations of a criminal nature which replace the "old" smuggling offences (defined in the aforementioned Presidential Decree no. 43/1973).

With particular reference to smuggling offenses, Legislative Decree 141/2024, innovating the provisions of the previous TULD, aimed to distinguish between criminal offenses and administrative offenses based on the objective criterion of the amount of fees owed. In this sense, the same decree, after defining the criminal offenses, provides in Article 96 that – where the offense is not aggravated by the occurrence of certain specific circumstances listed in Article 88[7] – The violations referred to in the previous articles 78 to 83 constitute a simple administrative offence rather than a crime if none of the boundary rights considered separately (whether due or unduly requested for restitution) exceeds the amount of 10,000 euros..

Art. 25-sexiesdecies
Smuggling

1. In relation to the commission of the crimes provided for by the national provisions supplementing the Union Customs Code, pursuant to the Legislative Decree issued pursuant to Articles 11 and 20, paragraphs 2 and 3, of Law No. 111 of 9 August 2023, and by the consolidated text of the legislative provisions concerning taxes on production and consumption and related criminal and administrative sanctions, pursuant to Legislative Decree No. 504 of 26 October 1995, a pecuniary sanction of up to two hundred quotas shall apply to the entity.
2. 2. When the taxes or border duties due exceed one hundred thousand euros, a pecuniary sanction of up to four hundred quotas is applied to the entity.
3. In the cases provided for in paragraphs 1 and 2, the interdictory sanctions provided for in article shall apply to the entity9, paragraph 2, letters c), d) and e) and, only in the case provided for in paragraph 2, also the interdictory sanctions provided for in article 9, paragraph 2, letters a) and b).

21. Crimes against cultural heritage and against cultural and landscape assets (articles 25-*septiesdecies*and 25-*twelve times*of the Decree)

Art. 25 septiesdecies

[7]The conduct may be considered criminally relevant (and, therefore, capable of causing the entity to incur liability pursuant to Legislative Decree 231/2001) only on condition that, alternatively:

- the fact is aggravated by one of the circumstances referred to in Article 88, paragraph 2, letters a) to d) of Legislative Decree no. 141/2024, namely:
  a) when, while committing the crime or immediately afterwards, in the surveillance area, the perpetrator is caught with a gun;
  b) when, while committing the crime or immediately afterwards, in the surveillance zone, three or more persons committing smuggling are caught together and in conditions such as to hinder the police;
  c) when the act is connected with another crime against public faith or against public administration;
  d) when the perpetrator is an associate to commit smuggling crimes and the crime committed is one of those for which the association was formed.
- the amount of at least one of the boundary fees owed or unduly collected, considered separately, or of the boundary fees unduly requested for reimbursement, exceeds €10,000.

Crimes against cultural heritage

1. In relation to the commission of the crime provided for in Article 518-novies of the Criminal Code, a pecuniary sanction of between one hundred and four hundred shares shall apply to the entity.
2. In relation to the commission of the crimes provided for in Articles 518-ter, 518-decies and 518-undecies of the Criminal Code, the pecuniary sanction of between two hundred and five hundred shares shall apply to the entity.
3. In relation to the commission of the crimes provided for in Articles 518-duodecies and 518-quaterdecies of the Criminal Code, the pecuniary sanction of between three hundred and seven hundred shares shall apply to the entity.
4. In relation to the commission of the crimes provided for in Articles 518-bis, 518-quater and 518-octies of the Criminal Code, the pecuniary sanction of between four hundred and nine hundred shares shall apply to the entity.
5. In the event of a conviction for the crimes referred to in paragraphs 1 to 4, the interdictory sanctions provided for in Article 9, paragraph 2, shall apply to the entity for a period not exceeding two years.

Art. 25-duodevicies
Recycling of cultural heritage and devastation and plundering of cultural and landscape heritage

1. In relation to the commission of the crimes provided for in Articles 518-sexies and 518-terdecies of the Criminal Code, the entity shall be subject to a pecuniary sanction ranging from five hundred to one thousand shares.
2. If the entity or one of its organizational units is used on a permanent basis for the sole or primary purpose of enabling or facilitating the commission of the crimes indicated in paragraph 1, the sanction of permanent disqualification from exercising the activity pursuant to Article 16, paragraph 3, shall apply.

Art. 25-undevicies
Crimes against animals

1. In relation to the commission of the crimes provided for by articles 544-bis, 544-ter, 544-quater, 544-quinquiese and 638 of the penal code, the pecuniary sanction of up to five hundred shares shall apply to the entity.
2. In the event of conviction or application of the penalty at the request of the parties, pursuant to Article 444 of the Code of Criminal Procedure, or of a criminal conviction decree, pursuant to Article 459 of the Code of Criminal Procedure, for the crimes referred to in paragraph 1 of this Article, the interdictory sanctions provided for in Article 9, paragraph 2, of this decree shall apply to the entity for a period not exceeding two years.
3. Paragraphs 1 and 2 do not apply to the cases provided for in Article 19-ter of the coordination and transitional provisions for the Criminal Code.


AUTO BANK

ANNEX B: Guidelines from Confindustria, Assilea, ASSOFIN, and ABI

In preparing this Model, the Company was inspired by the Guidelines of Confindustria, Assilea and ASSOFIN, which are briefly reported below.

Confindustria Guidelines

The key points that the Guidelines identify in the construction of the Models can be summarised as follows:

- Identification of the risk **areas**, aimed at verifying in which company area/sector the commission of crimes is possible.
- Establishment of a control system capable of preventing risks through the adoption of specific procedures.

The most relevant components of the control system designed by Confindustria are:

- code of ethics;
- organizational system;
- manual and computerized procedures;
- authorization and signature powers;
- control and management systems;
- communication to staff and their training.

The components of the control system must be inspired by the following principles:

- verifiability, documentability, coherence and congruence of each operation;
- application of the principle of separation of duties (no one can independently manage an entire process);
- inspection documentation;
- provision of an adequate sanctioning system for violations of the rules of the code of ethics and the procedures set out in the Model.
- Identification of the requirements of the supervisory body, which can be summarised as follows:
- autonomy and independence;
- professionalism;
- continuity of action;
- integrity and absence of conflicts of interest.
- Characteristics of the Supervisory Body (composition, function, powers, etc.) and related information obligations.

To ensure the necessary autonomy of initiative and independence, it is essential that the Supervisory Body is not assigned operational tasks that, by making it involved in decisions and operational activities, would undermine its objectivity of judgment when verifying conduct and the Model.

The Guidelines allow for both single- and multi-member compositions. The choice between one or the other solution must take into account the objectives pursued by the law and, therefore, must ensure effective controls in relation to the size and organizational complexity of the entity.

In a multi-member composition, internal and external members may be appointed to the Supervisory Body, provided that each meets the aforementioned autonomy and independence requirements. Conversely, in a mixed composition, since internal members cannot be expected to be completely independent from the body, the Confindustria Guidelines require that the body's degree of independence be assessed as a whole.

With regard to legal expertise, given that the legislation in question is essentially criminal law and the Supervisory Body's activity is aimed at preventing the commission of crimes, knowledge of the structure and methods of committing such crimes is essential. This knowledge can be provided to the Supervisory Body through the use of company resources or external consultancy.

In this regard, with regard to issues relating to health and safety at work, the Supervisory Body must make use of all the resources activated to manage the relevant aspects (as mentioned, RSPP – Head of the Prevention and Protection Service, ASPP – Prevention and Protection Service Workers, RLS – Workers' Safety Manager, MC – Competent Doctor, first aid workers, and emergency responders in the event of a fire).

Possibility, within corporate groups, of organizational solutions that centralize the functions required by Legislative Decree 231/01 at the parent company, provided that:

- each subsidiary must have its own Supervisory Body (without prejudice to the possibility of assigning this function directly to the subsidiary's management body if it is small);
- it is possible for the Supervisory Body established at the subsidiary to make use of the resources allocated to the analogous body of the Parent Company;
- When carrying out checks at other Group companies, the employees of the Parent Company's Supervisory Body act as external professionals who perform their activities in the interest of the subsidiary, reporting directly to the subsidiary's Supervisory Body.

Assilea Guidelines

Reference was also made to the "Guidelines for the Development of Organization, Management, and Control Models for Financial Leasing and Leasing in General" developed by Assilea, applicable to entities engaged in leasing activities. The Guidelines, similar to the Guidelines prepared by Confindustria, provide:

a. the analysis of Legislative Decree 231/01 and the related criminal offences implemented to date;

b. the requirements for the Supervisory Body and the possible options for identifying a structure to which the tasks set forth in Legislative Decree 231/01 can be entrusted (an internal body characterized by autonomy, independence, professionalism, and continuity of action. This autonomy presupposes that the Supervisory Body, in carrying out this function, is accountable only to the highest hierarchical level);

c. some recommendations for the construction of the Model (similar to those indicated in the Confindustria Guidelines).

Furthermore, they are based on principles and methodologies similar to those set out in the Confindustria Guidelines.

Guidelines of the Italian Association of Consumer and Real Estate Credit (ASSOFIN)

Since ASSOFIN is the trade association representing CA Auto Bank S.p.A., in preparing this Organization, Management and Control Model (hereinafter "Model"), the Company has taken inspiration from the Guidelines prepared by it.

These Guidelines provide:

- the analysis of Legislative Decree 231/2001 and the related criminal offences implemented to date;
- the requirements for the Supervisory Body and possible options for identifying a structure to which the tasks set forth in Legislative Decree 231/2001 can be entrusted; - some recommendations for the construction of the Model.

For each type of crime, ASSOFIN provides an indication of the individuals within the company who are most likely to commit them, listing some examples and the preventive controls to be introduced within the processes where the risk is most likely to arise.

The Guidelines also provide the minimum principles that must be contained in the company's code of ethics and the sanctioning mechanisms to be implemented against company employees and self-employed workers/suppliers or other parties having contractual relationships with the company.

It is understood that the decision not to adapt the Model to certain indications in the Guidelines does not affect its validity. In fact, each Model, having to be drafted with reference to the specific circumstances of the Company, may well deviate from the Guidelines, which, by their very nature, are of a general nature.

Italian Banking Association (ABI) Guidelines - Self-Laundering

The Italian Banking Association's Guidelines regarding the crime of self-laundering, introduced into the catalog of crimes by Law 186 of 2014, were also taken into consideration. Specifically, according to ABI, the new crime requires updating sensitive processes in Model 231 to prevent companies from acting in a way that hinders the identification of the (possible) illicit origin of assets. ABI's position, therefore, is to update the Model by focusing on the company's financial flow management system, identified as the process designed to prevent obstacles to the identification of the origin of assets. It should also be noted that the Guidelines issued by Assilea, cited above, also refer to the ABI Guidelines.

ANNEX C: Appendix

Please refer to the Excel file adopted by the Company and called “Appendix”, which indicates, in relation to the Sensitive and Instrumental Processes listed in this Model and falling within a specific Family of Crimes:

- the Company Functions / Departments involved;
- internal processes and related company procedures.

ANNEX D: Information flows to the Supervisory Body

Sensitive Process /Instrumental	**Reference in the Special Part**	**Flow description**	**Timings**
***Customer Relationship Management Management of activities*remarketing**	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority	Communicate, without delay, to your line manager or to the *management of* the Company and, at the same time, to the Supervisory Body any conduct carried out by those working for the counterparty, aimed at obtaining favors, illicit donations of money or other benefits, even towards third parties, as well as any critical issues or conflicts of interest that arise within the scope of the relationship.	At the event
Management of administrative obligations, relations with Supervisory Authorities and related inspection activities	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority	Communicate, without delay, to your line manager or to the *management* of the Company and, together with the Supervisory Body, any conduct carried out by those who operate with the public counterpart, aimed at obtaining favors, illicit donations of money or other benefits, including towards third parties, as well as any critical issues or conflicts of interest that arise within the context of the relationship with the Public Administration.	At the event
		Promptly report any inspections received and/or in progress to the Supervisory Body, specifying: (i) the Public Administration carrying out the	At the event

		inspection; (ii) the participating entities; (iii) the subject of the inspection and (iv) the period in which it was carried out.	
		Send the minutes signed by the Public Authorities and containing provisions, sanctions, observations, etc. to the Chief Executive Officer and the Supervisory Body.	At the event
		Submit to the Supervisory Body, every six months, the list of delegations and powers of attorney granted to company representatives for the purpose of maintaining relations with the Public Administration.	Half-yearly
Litigation management and relations with the Judicial Authority and management of settlement agreements	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority	All Recipients must promptly notify the Supervisory Body, through the communication tools existing within the Company (or with any communication tool, provided that it complies with the principle of traceability), of any action, summons to testify, and legal proceedings (civil, criminal, or administrative) that involve them, in any respect, in relation to the work performed or in any way related to it.	At the event
Management of purchases of goods and services (including consultancy)	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority Section 2.12 - Sensitive	Report to the Supervisory Body: or requests for unusually high fees; the requests for expense reimbursements that are not adequately documented or are unusual for the operation in question.	At the event

	Processes in the Area of Tax Crimes		
Selection and management ofpartnercommercial	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority	Communicate promptly to your line manager or to the *management* of the Company and, at the same time, to the Supervisory Body, also through the communication tools existing within the Company, any suspicious behavior or activities carried out by those working for the counterparty.	At the event
Financial flow management ***Management and evaluation of customer credit*** ***Management of intercompany relationships***	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others not to make statements or to make false statements to the Judicial Authority Section 2.12 - Sensitive Processes in the Area of Tax Crimes	Communicate, without delay, to the *management* company and, at the same time, the Supervisory Body, any critical issues that may arise within the scope of the activity in question.	At the event
		Report to the Supervisory Body, on a six-monthly basis, the results of the checks carried out on incoming and outgoing financial flows, indicating any anomalies found (for example, lack of supporting documentation, flows relating to purposes not related to the company's activity, etc.).	Half-yearly
Management of gifts, donations, events and sponsorships	Section 2.1 - Sensitive Processes in the context of crimes against the Public Administration and crimes of inducing others	To predict a report/periodical to be sent to the Supervisory Body regarding gifts, events, sponsorships and loans.	Annual

	not to make statements or to make false statements to the Judicial Authority		
Management of commercial relationships with customers, management of business activities*remarketing *and the management and evaluation of customer credit	Section 2.12 - Sensitive Processes in the Area of Tax Crimes	Communicate, without delay, to the *management company* and, at the same time, the Supervisory Body, any critical issues that may arise within the processes under examination.	At the event
Management of expense reports and entertainment expenses	Section 2.12 - Sensitive Processes in the Area of Tax Crimes	Communicate, without delay, to your line manager or to the *management of* the Company and at the same time to the Supervisory Body any behavior aimed at obtaining an illicit advantage for the Company.	At the event
Accounting management, budget preparation and tax management	Section 2.12 - Sensitive Processes in the Area of Tax Crimes	Report to your line manager or company management and, at the same time, to the Supervisory Body, both the existence of errors or omissions in the accounting process of management events and behaviors that do not comply with the above provisions.	At the event