knowledge
intensive
business
services

LATTANZIO KIBS S.p.A. Benefit Corporation

ORGANIZATIONAL, MANAGEMENT AND CONTROL MODEL
pursuant to Legislative Decree 231/2001

This is an English translation of the original document titled “Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001”. For any interpretation and legal purpose, the original version in Italian of this document is the only one with legal effect.

LATTANZIO KIBS

Index

ATTACHMENTS

- **Annex 1**: List of offenses
- **Annex 2**: Code of Ethics
- **Annex 3**: Organizational Chart

REVISION STATUS

REVISION NUMBER AND DATE	REVISION OBJECT
REV 00 - September 29, 2020	First version
REV 01 - May 10, 2021	First revision
REV 02 - June 23, 2023	Second revision
REV 03 - November 29, 2023	Third revision

1. INTRODUCTION BY LATTANZIO KIBS S.p.A. BENEFIT CORPORATION.

Lattanzio KIBS S.p.A. Benefit Corporation (hereinafter also referred to as "LKIBS" or the "Company"), a subsidiary of Lattanzio Group S.r.l., is Italy's leading boutique public sector consulting firm active in the global market (www.lattanziokibs.com).

Since its origins, Lattanzio KIBS has been dedicated to the modernization of PA as an engine of economic and social development to generate innovation in various policy areas, enhance administrative capacity, improve the quality of services to citizens and businesses, and implement projects that foster the growth of country systems.

In now 25 years of planning, Lattanzio KIBS has gained know-how in Italy at all levels of the institutional chain (ministries, regions, local authorities) and around the world in more than 100 countries alongside national and local governments, on assignments from the European Commission, the United Nations, the World Bank and major international development cooperation bodies.

The term KIBS, an acronym for knowledge-intensive business services, expresses the offering of different consulting 'practices' integrated in the activity of project analysis, development, implementation, evaluation, and dissemination, through which the Company is able to augment the required skill set and present innovative solutions with approaches, methodologies, and tools natively shared internally for strategic decision support.

Since 2016, through its business, Lattanzio KIBS has been committed to supporting sustainable development towards the SDGs (Sustainable Development Goals) of the United Nations 2030 Agenda, and since 2017 - among the first companies in Italy - has joined the United Nations Global Compact in support of the principles set by the UN to promote a sustainable economy that is respectful of human and labor rights, environmental protection and the fight against corruption.

In 2022, the Company amended its Articles of Incorporation by adopting the status of a Benefit Corporation for the purpose of combining the purpose of profit with specific purposes of common benefit in the exercise of its economic activity, operating responsibly, sustainably, and transparently towards its stakeholders. As a Benefit Corporation, Lattanzio KIBS aims to create social value from its historical vocation, namely:

- in institutions and public administrations to accelerate the modernization of the public sector with their own activities;
- in the education system and the labor market to orient talented young people to engage from the outside through counseling for the public sector;
- in their organization to encourage socially responsible forms of management.

Lattanzio KIBS believes that the principles of honesty, integrity and social responsibility-as codified in the internal rules of self-discipline and in the laws in force-are criteria conditioning the evaluation of its activities, on a par with its operating results.

Therefore, the Company adopts an Organization, Management and Control Model in order to adapt its organizational and control system to the provisions of Legislative Decree 231/2001.

2. FOREWORD

2.1. Normative Context of Reference

Legislative Decree No. 231 of June 8, 2001, having as its object the "Discipline of the administrative liability of legal persons, companies and associations, including those without legal personality" (hereinafter referred to as the "Legislative Decree 231/2001" or simply the "Decree"), introduced the liability of Entities, for administrative offenses dependent on crime, into our system.

This is a particular form of liability referred to as "administrative" which, in reality, takes the form of criminal liability on the part of entities, as it is established before a criminal court.

The Decree constitutes a far-reaching regulatory and cultural intervention in which, in addition to the criminal liability of the individual who committed the crime, the liability of the Entity for whose benefit or in whose interest the same crime was perpetrated is added.

The provisions contained in the Decree under Article 1, Paragraph 2, apply to the following "Subjects."

- Entities provided with legal personality;
- Companies and associations, including those without legal personality.

Pursuant to Subsection 3 below, however, they remain excluded from these regulations:

- the state;
- territorial public bodies;
- The other non-economic public bodies;
- Entities that perform functions of constitutional importance.

Liability is, therefore, attributed to the Entity if the offenses, indicated by the Decree and listed in the list attached to this Model (see Attachment No. 1 "List of Offenses"), are committed in its interest or advantage by:

- individuals who hold positions of representation, administration or management of the Entity or one of its organizational units with financial and functional autonomy, and those who exercise de facto management and control of the Entity (so-called "top individuals");
- persons subject to the direction or supervision of top management (so-called "subordinates").

With regard to the notion of "interest," it is embodied whenever the illegal conduct is carried out with the exclusive intention of achieving a benefit to the Entity, regardless of whether this objective is achieved.

Likewise, liability is incumbent on the Entity whenever the perpetrator of the offence, although not having acted for the purpose of benefiting the Entity, has nonetheless gained an "advantage" for the legal person, whether economic or otherwise.

A characteristic aspect of Legislative Decree 231/2001 is the attribution of an "exempting" value to the Organization, Management and Control Models adopted by Entities.

In fact, the Entity is not liable for offenses committed in its interest or to its advantage by one of the apical persons if it proves that:

- the management body has adopted and effectively implemented an Organization, Management and Control Model suitable for preventing the crimes covered by the Decree;
- the task of supervising the operation of and compliance with the Models and ensuring that they are updated has been entrusted to a "body" with autonomous powers of initiative and control;
- the crime relevant under the Decree was committed by fraudulently circumventing the Organizational Model;
- the crime was committed without there being failure or insufficient supervision by the body.

In this regard, organization and management models must meet the following requirements:

a) Identify the activities within the scope of which crimes may be committed;
b) Provide specific protocols aimed at planning the formation and implementation of the entity's decisions;
c) Identify ways of managing financial resources suitable for preventing the commission of crimes;
d) Provide for information obligations to the body responsible for supervising the operation of and compliance with the models;
e) Introduce an appropriate disciplinary system to punish non-compliance with the measures specified in the model.

Conversely, in the case of an offense committed by subordinates, the Entity will be liable where the commission of the offense was made possible by failure to comply with management and supervisory obligations.

Otherwise, liability is expressly excluded where the Entity has adopted, in relation to the nature and size of the organization as well as the type of activity carried out, "appropriate measures to ensure that the activity itself is carried out in compliance with the law" and to verify and discover and eliminate risk situations in a timely manner; as well as, where the aforementioned individuals have acted "in their own exclusive interest or that of third parties" (Art. 5, para. 2, Legislative Decree 231/01).

The administrative liability of the Entity is independent of the criminal liability of the natural person who committed the crime and stands alongside the latter.

Any imputation to the Entity of liability arising from the commission of one or more of the cases referred to in the Decree does not exclude the personal liability of the person who engaged in the criminal conduct.

Article 9 paragraph 1 of the Decree identifies the sanctions that can be imposed on the Entity, namely:

- financial penalties;
- disqualifying sanctions;
- Forfeiture of the price or profit of the crime;
- The publication of the judgment.

Financial penalties are calculated through a system based on quotas, which are determined by the court in number and amount within legally defined limits, taking into account:

- Of the seriousness of the fact;
- Of the degree of accountability of the Entity;
- of the activity carried out by the Entity to eliminate or mitigate the consequences of the act and to prevent the commission of further offenses;
- Of the economic and asset conditions of the Entity.

Disqualifying sanctions that may consist of:

- Disqualification from engaging in activities;
- suspension or revocation of authorizations, licenses or concessions functional to the commission of the offense;
- Prohibition of contracting with the public administration, except to obtain the performance of a public service;
- Exclusion from benefits, financing, contributions or subsidies and possible revocation of those already granted;
- Ban on advertising goods or services;
- commissioning.

Disqualification sanctions are also applicable as a precautionary measure, exclusively if at least one of the following conditions is met:

a) the Entity has derived a significant profit from the crime and the crime was committed by individuals in a senior position, or by individuals subject to the direction and supervision of others when the commission of the crime was determined or facilitated by serious organizational deficiencies;

b) In case of repeated offenses.

The aforementioned sanctions can be applied to the Entity exclusively by the Criminal Court and only if all the objective and subjective requirements set by the Legislature are met: the commission of a specific crime, in the interest or to the advantage of the company, by qualified individuals (apical or subordinate to them) and the assessment of the unsuitability of the organizational model applied or its failure to be implemented.

The liability of entities also extends to crimes committed abroad, provided that the state of the place where the act was committed does not proceed against them, provided that the special conditions set forth in Legislative Decree 231/2001 are met.

Legislative Decree 231/2001, as subsequently amended and supplemented, thus introduced the new regulations on the administrative liability of the Entity for certain crimes committed in its interest or to its advantage by individuals (and their subordinates) who exercise (de jure or de facto) representative, administrative and management functions.

The Entity's liability does not arise from the commission by the individuals just identified of any criminal offence, but is limited to the offence hypotheses, originally provided for by the Decree and subsequent intervening amendments, listed below:

a) crimes committed in relations with the Public Administration (Articles 24 and 25 of Legislative Decree 231/2001);

b) Computer crimes and unlawful data processing (Article 24-bis of Legislative Decree 231/2001);

c) organized crime offenses (Article 24-ter of Legislative Decree 231/2001);

d) Crimes in the area of counterfeiting money, public credit cards, revenue stamps and identification instruments or signs (Article 25-bis of Legislative Decree 231/2001);

e) crimes against industry and trade (Article 25-bis.1 of Legislative Decree 231/2001);

f) corporate crimes (Article 25-ter of Legislative Decree 231/2001);

g) crimes for the purpose of terrorism or subversion of the democratic order (Article 25-quater of Legislative Decree 231/2001);

h) crimes against the individual (Article 25-quinquies of Legislative Decree 231/2001) and crimes consisting of female genital mutilation practices (Article 25-quater.1 of Legislative Decree 231/2001);

i) market abuse offenses (Article 25-sexies of Legislative Decree 231/2001 and Article 187-quinquies TUF);

j) Crimes of culpable homicide and grievous or very grievous bodily harm committed in violation of the regulations on health and safety in the workplace (Article 25-septies of Legislative Decree 231/2001);

k) the crimes of receiving stolen goods, money laundering, use of money, goods or benefits of illicit origin, and self-laundering (Article 25-octies of Legislative Decree 231/2001);

l) Crimes related to non-cash payment instruments (Article 25-octies.1 of Legislative Decree 231/2001)

m) Copyright infringement offenses (Article 25-novies of Legislative Decree 231/2001);

n) crime of inducement not to make statements or to make false statements to judicial authorities (Article 25-decies of Legislative Decree 231/2001);

o) Environmental crimes (Art. 25-undecies of Legislative Decree 231/2001);

p) crime of employment of third-country nationals whose stay is irregular (Article 25-duodecies of Legislative Decree 231/2001);

q) crime of bribery among private individuals (Art. 25-ter, I C., letter S-bis) of Legislative Decree 231/2001);

r) Racism and xenophobia crimes (Article 25-terdecies of Legislative Decree 231/2001);

s) fraud in sports competitions, abusive gaming or betting and gambling exercised by means of prohibited devices (Article 25-quaterdecies of Legislative Decree 231/2001);

t) tax crimes (Article 25-quinquesdecies of Legislative Decree 231/2001);

u) smuggling (Article 25-sexiesdecies of Legislative Decree 231/2001);

v) crimes against cultural heritage (Article 25-septiesdecies of Legislative Decree 231/2001);

w) offenses related to laundering of cultural property and devastation and looting of cultural and scenic property (Art. 25-duodevicies of Legislative Decree 231/2001);

x) transnational crimes (L. 146/2006).

With reference to the offenses listed generically above, they are detailed and explained in Annex 1 for the sake of better clarity.

2.2. Structure of the Model

The Organization, Management and Control Model prepared and adopted by LKIBS (hereinafter also referred to as the "Model" or "Model 231," consists of:

- a General Part that provides an overview of the overall system of principles, organizational rules and control tools adopted by LKIBS to prevent the commission, within the scope of its activities, of the crimes relevant under Legislative Decree 231/01 and to ensure the transparency, legality, fairness and consistency of its actions. A section of the General Part is devoted to the Supervisory Board (SB), where its duties, functions and powers are described, and a further section concerns the system of sanctions to be applied in case of the commission of offenses;
- different Special Sections that describe, for each area of business activity for which the crimes provided for in the Decree are potentially feasible, the relevant offenses, the behavioral principles to be observed, as well as the control garrisons that all persons, operating within LKIBS or in relations with it, are required to apply in order to avoid the occurrence of administrative liability of the Company and to prevent the commission of the crimes relevant under the Decree.

Art. 6, co. 3, Legislative Decree 231/2001 provides that "organizational and management models may be adopted, guaranteeing the requirements of paragraph 2, on the basis of codes of conduct drawn up by the associations representing the entities, communicated to the Ministry of Justice, which, in consultation with the competent ministries, may make observations within thirty days on the suitability of the models to prevent crimes."

This Model has been prepared taking into account the indications expressed in the guidelines developed by Confindustria and approved by the Ministry of Justice.

They constitute Annexes to the Model:

- The List of predicate offenses for the administrative liability of companies and entities under Legislative Decree 231/2001 (Annex 1);
- The Code of Ethics (Appendix 2).

The Administrative Body of LKIBS undertakes - at the indication of the SB - to supplement the Model in the event of subsequent regulatory interventions that change the types of offenses or assume relevance for the application of the regulations on the administrative liability of entities or in the event of significant changes in the organizational structure of LKIBS.

2.3. Purpose of the Model

The adoption of the Model constitutes a valuable tool to raise awareness among the Recipients of the same, so that they follow, in the performance of their activities, correct and straightforward behavior, such as to prevent the risk of commission of the offenses contemplated in the Decree.

The Company has decided to adopt this organization, management and control model (hereinafter the "Model") for the purpose of:

a) promote and enhance to an even greater extent an ethical culture internally, with a view to fairness and transparency in the management of activities, making all those who work in the name and on behalf of LKIBS, in areas of activity at risk, responsible;

b) Introduce a mechanism to establish a permanent process, albeit to be updated periodically, of analysis of the company's activities, aimed at identifying the areas in the scope of which the crimes indicated by the Decree may abstractly occur;

c) introduce control principles to which the organizational system must conform, so as to be able to prevent in practice the risk of commission of the crimes indicated by the Decree in the specific activities that emerged as a result of the activity of analysis of sensitive areas.

2.4. Addressees of the Model

The rules contained in this Model and its Annexes apply:

- To the Administrative Body;
- to Heads of Organizational Units (e.g. Head of Business Unit), all other employees and collaborators (collectively the "staff");
- to those who, although not belonging to the Company, act on its behalf (consultants, attorneys and, in general, all third parties acting on behalf of LKIBS).

Those to whom the Model is addressed are therefore required to comply with all of its provisions punctually, including in fulfillment of the duties of loyalty, fairness and diligence that arise from the legal relationships established with LKIBS.

Contracts/letters of engagement entered into with consultants/suppliers who carry out activities on behalf of or for the Company must include an appropriate clause (or provide for a broader statement on the side of the contract) in which the counterparty declares that it has received and understood the LKIBS Model 231 (including its annexes) and that it undertakes to adhere to and abide by the principles contained therein.

2.5. Approval, amendment and integration of the Model

The organization and management models constitute, pursuant to and for the purposes of Article 6 paragraph 1, letter a) of the Decree, acts of issuance of the Top Management. Therefore, the approval of this Model and its constituent elements constitutes the prerogative and exclusive responsibility of the Administrative Body of LKIBS. The formulation of any amendments and additions to the Model is the exclusive responsibility of the Administrative Body itself, including on the recommendation of the Supervisory Board, for the following elements (given by way of example):

- Changes in the Company's organizational structure and/or the way of conducting business activities;
- regulatory changes;
- audit findings;
- Significant violations of the requirements of the Model.

Changes in company procedures necessary for the implementation of the Model are made by the relevant Organizational Units. The Supervisory Board is constantly informed of the updating and implementation of new procedures and is entitled to express its opinion on proposed changes.

2.6. Implementation of the Model

The adoption of this Model is the starting point of the process of dynamically conducting the Model itself.

For the implementation phase of the Model, the Administrative Body and the Heads of Organizational Units are responsible, for their respective areas of responsibility, for the implementation of the various elements of the Model, including operational procedures.

In any case, LKIBS reiterates that the proper implementation and control over compliance with corporate provisions and, therefore, with the rules contained in this Model, constitute an obligation and duty of all Company personnel and, in particular, of each Head of Organizational Unit to which is entrusted, within the scope of its competence, the primary responsibility for the control of activities, especially those at risk.

3. GENERAL PART.

3.1. Organizational system of the Company

The Organizational System of LKIBS has been set up to be sufficiently formalized and clear, especially with regard to the allocation of responsibilities, lines of hierarchical dependence, and job descriptions, with specific provision for control principles such as, for example, the juxtaposition of functions.

The adequacy of this organizational system was verified based on the following criteria:

- Formalization of the system;
- Clear definition of assigned responsibilities and lines of hierarchical dependence;
- Existence of the opposition of functions;
- Correspondence between the activities actually performed and what is stipulated in the company's missions and responsibilities.

The organizational structure of LKIBS is formalized and graphically represented in an organizational chart, which clearly defines the lines of hierarchical dependence and functional links between the various positions of which the structure is composed.

It should be noted that, for the management of characteristic activities, LKIBS can also make use of resources belonging to other companies of the Lattanzio Group, based on the powers granted to individual directors, which in turn are regulated by a specific service contract.

The Organizational Chart and all related documents are subject to constant and timely updating as a result of any changes in the organizational structure.

The exact identification of each person's duties and their assignment in a clear and transparent manner enables compliance with the principle of separation of roles, which is necessary in order to curb the risk of the commission of crimes punishable under Legislative Decree 231/2001.

3.2. System of Internal Controls

The system of internal controls consists of procedural, governance and more strictly operational rules that regulate business processes, activities and related controls with the aim of:

- Ensuring compliance with corporate strategies;
- Ensure the effectiveness and efficiency of processes;
- Ensure the reliability and integrity of accounting and management information;
- Ensure compliance of operations with the law, plans, regulations and internal company procedures;
- ensure the level of compliance with UNI EN ISO 9001 and UNI EN ISO 14001, as well as all other certifications/attestations obtained by the Company (e.g. SA 8000, UNI EN ISO 27001, UNI/PDR 125, ISO 30415);
- make timely, organic, structured, and quantitative information available to management, enabling them to verify and compare the evolution of the level of quality achieved over time.

The system of internal controls is periodically subject to monitoring and adjustment in relation to changes in business operations and the relevant regulatory environment.

The system adopted by LKIBS consists of the following main elements:

- The formalized corporate organization that defines structure, roles, responsibilities, authorizing powers and hierarchical dependencies;
- The set of procedures referring to different business processes;
- the corporate information system ("dashboard") that manages all significant procedural flows of the company, guiding employees in following company procedures and providing management with a management database necessary for running the company;

- service orders and internal regulations governing the performance of internal activities and ensuring the traceability and documentability of transactions and controls performed, in compliance with the principle of separation of functions and ensuring that every transaction or action is verifiable, documented, consistent and congruent;
- A system for managing financial resources and payments;
- A training and information system, aimed at raising awareness and dissemination at all levels of the company of the ethical principles and rules of conduct, the procedures issued and the contents of the Organization, Management and Control Model;
- The Code of Ethics, which defines the general ethical values and principles to which the corporate bodies and their members as well as the Company's employees, collaborators and consultants must be inspired in the conduct of their activities, in order to prevent the occurrence of unlawful conduct or conduct not aligned with corporate standards;
- A disciplinary system that takes action in case of non-compliance with the provisions of the Code of Ethics, operating procedures and the Organization, Management and Control Model.

The Organizational Unit in charge of compliance audits (Compliance and Quality) oversees the adequacy and reliability of the company's System of Internal Controls and supports the Supervisory Board in matters pertaining to "231" aspects.

3.3. The construction of LKIBS' Model 231.

The process of constructing the Model (and any subsequent revisions that became necessary) was developed through the design phases described below.

1. Identification of the activities and processes within the scope of which the conditions, occasions and/or means for the commission of the crimes provided for in the Decree ("sensitive activities") could potentially occur, as well as the Organizational Units involved in the performance of these activities.
2. Analysis of sensitive activities and processes and survey of organizational and control mechanisms in place or to be adapted. The control system was examined by considering the following standard prevention safeguards:
    - Existence of formalized procedures;
    - Ex-post traceability and verifiability of transactions through appropriate documentary/information supports;
    - existence of a system of formalized powers and authorization levels consistent with assigned organizational responsibilities;
    - Compliance with the principle of separation of duties;
    - Existence of appropriate specific control and monitoring mechanisms.
3. Upon completion of the activities described above, development (and, subsequently, updating) of the Company's Model, articulated according to the guidelines contained in the Guidelines issued by Confindustria.

The Model thus structured (and any subsequent revisions) is finally implemented through: a) its approval by the Administrative Body; b) the appointment/renewal of the Supervisory Board in charge of verifying the effective implementation and observance of the Model; c) the definition/updating of a disciplinary system against any violations of the Model; d) the dissemination of the Model's contents through training and information activities for Recipients.

3.4. Code of Ethics

The adoption of ethical principles relevant to the prevention of crimes under Legislative Decree 231/2001 is a primary objective of this Model. In this perspective, the adoption of a Code of Ethics as a useful governance

tool constitutes an essential element of the preventive control system. The Code of Ethics, in fact, aims to recommend, promote or prohibit certain behaviors.

The Code of Ethics has as its main objective the clear definition of fundamental ethical values and contains the general principles that should inspire the behavior of corporate bodies and their members, employees and collaborators and consultants of the Company.

The Code of Ethics adopted by all Group companies and LKIBS is attached to this Model and forms an integral part of it (see Attachment No. 2 "Code of Ethics").

The LKIBS Code of Ethics is addressed to the Administrative Body and employees, but it also extends to consultants, collaborators, attorneys and third parties acting on behalf of the Company. The Code's enforceable effect is, therefore, also directly applicable to those parties with respect to whom compliance with ethical principles may be contractually agreed.

Any doubts about the application of the principles and rules contained in the Code of Ethics should be promptly discussed with the Supervisory Board.

Anyone who becomes aware of violations of the principles of the Code or other events likely to alter its scope and effectiveness is required to promptly report them to the Supervisory Board.

Failure to comply with the principles and rules of conduct contained in the Code will result in the application of the sanctions provided for in the Company Disciplinary System set forth in the Model.

3.5. Training and Communication

3.5.1. Training

Internal training is an indispensable tool for effective implementation of the Model and widespread dissemination of the principles of behavior and control adopted by the Company, in order to reasonably prevent crimes, from which the Decree triggers administrative liability.

This training activity takes place after the adoption of the Model on the initiative of the Administrative Body and the Company's designated structures, through the exposition of the fundamental criteria of the administrative responsibility of the Entity, the crimes taken into account by the decree, as well as the type of sanctions provided for and the contents of the adopted Model.

The Supervisory Board verifies that personnel training, regarding the application of the Organization, Management and Control Model, is adequate and consistent with regulatory provisions, as well as with the provisions of the Model itself.

Training programs are shared with the Supervisory Board.

The requirements of the training program are as follows:

- Appropriateness with respect to the function held by the individuals within the organization;
- periodicity defined as a function of (i) the degree of change to which the external environment in which the company acts is subject to change, (ii) the learning capacity of the staff, and (iii) the degree of management's commitment to lend authority to the training activity carried out;
- selection of competent and authoritative speakers in order to ensure the quality of the content covered, as well as to highlight the importance of the training in question for the Company and the strategies it wishes to pursue;
- Mandatory participation (with appropriate control mechanisms to monitor attendance of subjects);
- Monitoring and verification of attendance and the degree of learning of participants.

In the event of significant changes and/or updates to the Model, in-depth modules are organized aimed at learning about the changes that have occurred.

Lastly, specific modules are organized for new hires to work in risk areas.

3.5.2 Communication

In line with the provisions of Legislative Decree 231/2001, the Company gives full publicity to this Model in order to ensure that all Recipients are aware of all its elements.

Communication is always thorough, effective, clear and detailed, with periodic updates related to changes in the Model.

The actual communication plan regarding the essential components of this Model is developed, consistent with the principles defined above, with communication to all Recipients through the means of communication deemed most appropriate, such as, for example, the use of e-mail, publication on the company's intranet site (dashboard), and/or personalized sending of appropriate communication.

3.6. Supervisory Board

Pursuant to Article 6 of Legislative Decree No. 231/2001, one of the necessary conditions for the Company not to be liable for offenses committed by its staff or appointees is to have entrusted the task of supervising the operation, effectiveness and compliance with the Model to a special Body, endowed with autonomous powers of initiative and control.

Legislative Decree 231/2001 does not provide specific indications regarding the composition of the Supervisory Board. In the absence of such indications, the Company has opted for a solution that, taking into account the purposes pursued by the law and the guidelines obtainable from published case law, is capable of ensuring, in relation to its size and organizational complexity, the effectiveness of the controls to which the Supervisory Board is assigned.

The Company has opted for a collegial composition of its Supervisory Board (hereinafter also the "SB").

3.6.1 General principles on the establishment, appointment and replacement of the Supervisory Board

The Company's Supervisory Board is established by resolution of the Administrative Body on the recommendation of the Shareholders' Meeting.

The SB remains in office for a period of time deliberated by the Governing Body and its composition can be confirmed at the end of the term.

The Supervisory Board ceases due to the expiration of the term established at the time of its appointment, although it continues to perform its functions on an interim basis until a new appointment of the Board, which must be made by the first useful resolution of the Administrative Body.

If, during the term of office, the Supervisory Board ceases to hold office, the Administrative Body shall replace it by its own resolution.

The compensation of the Supervisory Board is determined by the Administrative Body.

Based on Legislative Decree 231/2001, the Body to be entrusted with the task of supervising the Model must have the following requirements:

- Autonomy and independence: the SB must guarantee the autonomy of the control initiative from any form of interference or conditioning by any component of the Company. These requirements can be considered satisfied by providing for reporting to the top management of the company, i.e. to the Administrative Body or, when necessary, directly to the Shareholders' Meeting. In order to guarantee these requirements, moreover, it must not be assigned operational tasks that would undermine its objectivity of judgment in the exercise of its functions. In order to carry out its functions in absolute independence, the Supervisory Board has autonomous spending powers on the basis of an annual budget, approved by the Administrative Body on the proposal of the Body itself; in this way, the latter will be able to have an adequate endowment of financial resources for any need necessary for the proper performance of tasks and to cover the remuneration of the members of the Body. To safeguard the principle of autonomy and independence, those who are in situations of:
    - conflict of interest, even potential, with the Company such as to impair the independence required by the role and duties one would be performing;
    - of relationships of kinship, marriage, or affinity within the fourth degree with members of the Administrative Body, senior persons in general, auditors of the company and auditors appointed by the Auditing Company with members of the corporate bodies and with top management.
- Honorability: adequate "honorability" requirements must be possessed from the time of appointment as a member of the SB; according to this principle, those who:

- are in the conditions stipulated in Article 2382 of the Civil Code (disqualification, incapacitation, bankruptcy, conviction to the accessory penalty of disqualification, even temporary, from public office or inability to exercise executive offices);
- are under investigation or have been convicted, subject to the effects of rehabilitation, of one of the crimes among those to which Legislative Decree No. 231/2001 is applicable or crimes whose maximum sentence is more than 5 years. Conviction also means the sentence rendered pursuant to Article 444 of the Code of Criminal Procedure;
- have suffered the application of the ancillary administrative sanctions provided for in Article 187 quater of Legislative Decree No. 58/1998.

- Professionalism: in order to effectively carry out the functions entrusted to it, the SB must possess, a wealth of specialized knowledge, tools and techniques peculiar to those who carry out inspection and consultancy activities of control system analysis (business organization, finance, procedure analysis, etc.) and of a legal nature. Such techniques can be used:
  - on a preventive basis, to indicate possible and appropriate amendments to the Model in order to adopt the most appropriate measures to prevent the commission of crimes;
  - on an ongoing basis to verify compliance with codified behaviors with actual operations;
  - a posteriori, to ascertain how the crime could have occurred and who committed it.
  - With regard to legal competencies, and in particular criminal law, in order to be able to carry out the preventive activity for the realization of crimes, the SB must be familiar with the structure and methods of realization of crimes either through the use of internal company resources and/or external consulting.

  For these reasons, it is appropriate for the composition of the Supervisory Board to be collegial.
- Continuity of action: in order to ensure the effective and constant implementation of the model, it is necessary to have a structure dedicated to the activity of supervision of the Model, without operational duties that could lead it to take decisions that have economic-financial effects; however, this structure can provide advisory opinions on the construction of the model, at the stage of its drafting.

In order to guarantee the necessary stability to the members of the Supervisory Board, the revocation of the powers proper to the Supervisory Board and the attribution of such powers to another person may take place only for just cause, including those related to organizational restructuring interventions of the Company, through a special resolution of the Administrative Body and after consulting the Board of Auditors.

In this regard, "just cause" for revocation of the powers associated with the office of member of the Supervisory Board may mean, by way of example only:

- a final conviction of the Company pursuant to the Decree or a plea bargaining sentence, which has become final, where it expressly appears from the records "the omitted or insufficient supervision" by the Supervisory Board, according to the provisions of Article 6, paragraph 1, letter d) of the Decree;
- the failure of one or more of the above requirements of autonomy, independence or honorability;
- The violation of confidentiality obligations to which the SB is bound;
- Failure to attend more than two consecutive meetings without a justified reason;
- gross negligence in the performance of its duties such as, for example, failure to prepare the periodic information report to the Administrative Body on its activities;

3.6.2 Functions and powers of the Supervisory Board

The Supervisory Board is vested with the powers of initiative and control necessary to ensure effective and efficient supervision of the functioning and observance of the Model in accordance with the provisions of Article 6 of Legislative Decree 231/2001.

In particular, the SB must supervise:

- on the actual adequacy and effectiveness of the Model with respect to the need to prevent the commission of crimes for which Legislative Decree 231/2001 applies, also taking into account the size and organizational and operational complexity of the Company;
- On the permanence over time of the adequacy and effectiveness requirements of the Model;
- on compliance with the requirements of the Model by the Recipients, noting any violations and proposing the relevant corrective actions and/or sanctions to the competent corporate bodies;
- On updating the Model in the event that adjustment needs are found in relation to changed business or regulatory conditions, proposing any adjustment actions to the relevant corporate bodies and verifying their implementation.

For the performance and exercise of its functions, the SB is assigned the duties and powers of:

- access to all Company facilities and all relevant company documentation for the purpose of verifying the adequacy of and compliance with the Model;
- Carry out targeted spot checks on specific activities/operations at risk and on compliance with the control and behavior safeguards adopted and referred to in the Model;
- Promote the updating of risk mapping in the event of significant organizational changes or extension of the type of crimes taken into consideration by Legislative Decree 231/2001;
- Coordinate with the relevant Organizational Units to assess the adequacy of the adopted body of internal regulations and define any proposals for adaptation and improvement (internal rules, operating and control methods), subsequently verifying their implementation;
- Monitor information/training initiatives aimed at disseminating knowledge and understanding of the Model within the company;
- request from the Heads of Organizational Units, particularly those who work in company areas at potential risk of offenses, the information deemed relevant for the purpose of verifying the adequacy and effectiveness of the Model;
- Collect any reports from any Recipient of the Model regarding: i) any critical aspects of the measures provided for in the Model; ii) violations of the Model; iii) any situation that may expose the Company to the risk of crime.
- periodically report to the Administrative Body and the Heads of the Organizational Units concerned any violations of control principals referred to in the Model or the deficiencies detected during the audits carried out, so that they can take the necessary adjustment actions involving, where necessary, the Board of Directors;
- Supervise the consistent application of sanctions provided for in internal regulations in cases of violation of the Model, without prejudice to the competence of the management body for the application of sanction measures;
- Detect any behavioral deviations that may emerge from the analysis of information flows and reports to which the Recipients of the Model are bound.

The Supervisory Board may take advantage, under its direct supervision and responsibility, in carrying out the tasks entrusted to it, of the collaboration of all the structures of the Company or Lattanzio Group, or external consultants, making use of their respective skills and professionalism. This faculty allows the Supervisory Board to ensure a high level of professionalism and the necessary continuity of action.

The Supervisory Board adopts its own Rules of Procedure where, among other things, the scheduling and conduct of meetings and voting procedures are provided.

All members of the Supervisory Board are bound by a duty of confidentiality with respect to all information of which they become aware due to the performance of their duties.

Disclosure of such information may be made only to the individuals and in the manner prescribed by this Model.

It should be pointed out that the activities carried out by the SB cannot be reviewed by another internal body, but it is up to the Administrative Body to supervise the adequacy of its intervention, as it is likely to result in an

event capable of affecting the very functioning and effectiveness of the organizational model, since this responsibility ultimately rests precisely on the Administrative Body.

3.6.3 Reporting Activities

With regard to reporting activities, the SB reports to the Administrative Body and the Board of Auditors on the implementation of the Model and the emergence of any critical issues through two types of reporting:

- the first, semi-annually, to the Administrative Body in which the verification activities carried out and their outcome are reported;
- the second, annual, through which the activities carried out in the current year, together with the plan of activities for the following year, are presented to the Administrative Body and the Board of Auditors.

In case of extraordinary situations (such as receiving reports that are of an urgent nature, ascertaining that violations of the Model have occurred), the SB will immediately inform the Administrative Body.

If the SB detects a violation of the Model referable to the Administrative Body, it makes a report to be addressed promptly to the other members of the Body (if any), the shareholders and the Board of Auditors.

The interventions of the SB must be minuted and copies of the minutes must be kept. If critical issues are detected, they should be reported to one or more corporate bodies.

The SB meets at least 4 times a year, and minutes are taken of the meetings.

The SB has the power to request for urgent reasons the convening of the Administrative Body and the Board of Auditors, which, in turn, can convene, like the Administrative Body, the SB at any time.

3.6.4 Information obligations to the Supervisory Board

The Supervisory Board must be promptly informed by means of appropriate reports of acts, conduct or events that could result in a violation of the Model or illegal conduct that is relevant for the purposes of Legislative Decree 231/2001 of which the Recipients themselves have become aware by reason of the functions performed.

In particular, pursuant to paragraph 2-bis of Article 6 of Legislative Decree No. 231/2001, the Model must provide for internal reporting channels, the prohibition of retaliation as well as the disciplinary system adopted in this regard.

In this regard, the Company has adopted the **Whistleblowing Policy**, and all Recipients of this Model are obliged to promptly report the following information (so-called "reports"), in addition to any other violations under this policy:

- The commission, attempted commission, or reasonable danger of commission of the offenses under the Decree;
- any alleged violations of the behavioral and operational methods defined in the Code of Ethics, the Model or relevant company procedures, of which they have directly or indirectly become aware;

Reports should be made-as per the procedure stated in the Whistleblowing Policy-through the dedicated IT platform, which can be reached at the link https://lattanzio.whistlelink.com/.

Reports made through this platform are accessed exclusively by the "Report Manager" who keeps the Supervisory Board informed about them.

Through the platform, reports can be made:

- In written form, by filling out a form with a series of guided questions; or
- Orally, through a voice messaging system.

However, the reporter has the right to be heard/interviewed in person by the Reporting Manager upon his/her express request. In addition, the platform has a built-in messaging system for any exchange of information between the reporter and the Manager.

It is necessary for the report, which can also be anonymous, to be as substantiated as possible, as well as well-founded, in order to allow for verification and subsequent investigation.

The transmission of the report through the dedicated channel is carried out in accordance with the criteria of maximum confidentiality and privacy and in a manner suitable to protect the reporter, other protected subjects

under Legislative Decree 24/2023 and the identity and honorability of the reported subjects, without prejudice to the effectiveness of the subsequent investigation activities.

Bona fide whistleblowers are guaranteed against any form of retaliation, discrimination or penalization, direct or indirect, and in all cases the confidentiality of the whistleblower's identity is ensured, without prejudice to legal obligations and the protection of the rights of the Company or persons wrongly accused and/or in bad faith.

Please refer to the **Whistleblowing Policy** for more details regarding the protections and safeguards provided and the actions to be taken if you believe you have been retaliated against.

The reporting obligations of Model Recipients must be specified in special clauses included in the contracts that bind these individuals to LKIBS.

The Reporting Manager promptly evaluates the reports received and the cases in which it is necessary to take action, possibly including hearing from the reporter and/or the person responsible for the alleged violation.

Where the report pertains to areas concerning Model 231, the Supervisory Board must be promptly informed (by appropriately anonymizing the information) and must be updated at all stages of its handling. In addition, at the request of the Reporting Manager, it may provide support in the course of audits.

As part of the information flows required by Procedure 14 "Information Flows," the Whistleblowing Reporting Manager will, at least semiannually, prepare a report summarizing the reports received, the outcome of any analysis carried out and any ongoing analysis, and forward it to the Company's Supervisory Board.

They constitute sanctionable conduct, consistent with the provisions of the penalty system in Section 3.7 below:

- The commission, even attempted or threatened, of any retaliation against the whistleblower or other persons protected under Legislative Decree 24/2023;
- The commissioning of actions or behaviors designed to obstruct or attempt to obstruct reporting;
- The violation of the duty of confidentiality;
- The disruption of internal reporting channels;
- Failure to carry out verification activities regarding the reports received.

The conduct of the whistleblower in bad faith is also liable to disciplinary sanction, if it is established that the whistleblower is responsible, even by a judgment of first instance, for the crimes of defamation or slander (or otherwise for the same crimes committed in connection with whistleblowing) or his civil liability in cases of willful misconduct or gross negligence.

In addition to reports of specific violations, Heads of Organizational Units must promptly transmit to the SB information concerning:

- Measures and/or news concerning the existence of significant administrative or civil proceedings related to requests or initiatives of Public Authorities;
- requests for legal assistance made by Employees in the event of the initiation of any legal proceedings against them (not only in relation to offenses under Legislative Decree No. 231/2001);
- reports prepared by the Managers of other Organizational Units in the exercise of their functions and from which facts, acts, events or omissions with profiles of criticality with respect to compliance with the rules of the Decree could emerge;
- news about the sanctioning proceedings carried out and any measures imposed (including measures towards employees/employees/collaborators/consultants) or of the measures to dismiss such proceedings with the relevant reasons, if they are related to the commission of Offences or violation of the Model's rules of conduct or procedures;
- Summary schedules of contracts awarded as a result of tenders at the national and European level, or by private treaty;

- Summary schedules of contracts awarded by public agencies or entities performing public utility functions;
- information regarding decisions on the application for, disbursement, or use of public grants not from specific contracts.
- visits, inspections and investigations initiated by relevant public agencies and, upon their conclusion, any findings reported and penalties imposed;
- Any act or subpoena to testify involving individuals from the Company or working with it;
- Any information related to any work-related injuries and/or occupational diseases;
- Communications pertaining to organizational and corporate changes;
- any act, fact, event or omission detected or observed in the exercise of assigned responsibilities and duties with a profile of criticality with respect to the rules of the Decree;
- Observations on the adequacy of the control system;
- any behavioral exception or any unusual occurrence stating the reasons for the discrepancies and noting the different process followed.
- anomalies or critical issues encountered in the performance of sensitive activities for the application of Legislative Decree 231/2001;
- any additional information relevant to the compliance, operation and adaptation of Model 231.

In addition, employees and seconded persons must promptly notify the SB:

- measures and/or communications from Judicial Police organs, or any other Authority, from which it is inferred that investigations are being carried out for the Crimes, even against unknown persons, if such investigations involve LKIBS or its Employees or seconded or members of its Corporate Bodies.

In the charge of each Head of Organizational Unit involved in "sensitive" processes pursuant to Legislative Decree 231/2001, as the person in charge of the complete and correct adoption of the company rules to guard against the risks identified in the sectors under his or her jurisdiction, there is also the obligation to transmit to the Supervisory Board, on a periodic or event-driven basis, the data and information formally requested by the latter (c.d. "specific information".d. "specific information"), under procedure PR14 "Information flows and attestations to the Supervisory Board" to which reference is made.

Finally, with the periodicity established by the SB, the Managers of the Organizational Units involved in "sensitive" processes pursuant to Legislative Decree. 231/2001, by means of a process of self-diagnosis on the activity carried out, certify in a written statement, the level of implementation of the Model with particular attention to compliance with the principles of control and behavior and operating rules, reporting any critical issues and behaviors significantly different from those described in the process and the reasons that made it necessary or appropriate such deviation from the indications dictated by the Model or more ingenerally from the regulatory framework, as well as the adequacy of the remedial actions taken.

Periodic attestations are sent to the SB via e-mail to odvLKIBS@lattanziokibs.com.

All information, reports, reports provided for in the Model are kept by the Supervisory Board in a special confidential file (computer or paper). Access to said archive is allowed exclusively to the members of the Supervisory Board and only for reasons related to the performance of the tasks represented above.

The outgoing members of the Supervisory Board must ensure that the transfer of the management of the archive is properly passed on to the new members.

3.7. Penalty system

For the effectiveness of the organization, management and control model, it is essential to provide, for cases of violation of the ethical principles and the requirements and procedures set forth in the Model itself, an adequate system of sanctions, in accordance with the applicable CCNL and Article 7 of the Workers' Statute.

It should be noted that, in case of violations of the Model and the Code of Ethics, the application of the disciplinary system and related sanctions by the employer is independent of the conduct and outcome of any criminal proceedings initiated by the judicial authorities against the material author of the criminal conduct.

For seconded personnel, the power to impose disciplinary sanctions remains with the seconding company.

3.7.1 Penalties for employed or seconded non-management personnel

In the event of violation of the Model by non-managerial employees, or even by non-managerial personnel seconded to LKIBS, the following disciplinary measures, as provided for in Article 225 of the National Collective Bargaining Agreement for the tertiary, distribution and services industry, will apply:

a) Verbally inflicted reprimand for minor failures;

b) reprimand imposed in writing in cases of recurrence of the offenses referred to in (a) above;

c) Fine in an amount not exceeding the amount of 4 hours of normal pay;

d) Suspension from pay and service for up to 10 days;

e) Disciplinary dismissal without notice and with the other consequences of reason and law.

LKIBS will apply the measures in (a), (b), (c), (d), and (e) above depending on the seriousness of the conduct, i.e., in relation to the extent of the misconduct and the accompanying circumstances.

In particular, the application of sanctions must be guided by the principle of proportionality provided for in Article 2106 of the Civil Code, that is, it must be graduated according to the objective seriousness of the fact constituting a disciplinary offense. To this end, it will take into account:

- Of the intentionality of the behavior or the degree of guilt;
- of the employee's overall behavior with particular regard to the existence or absence of disciplinary history;
- of the level of responsibilitỳ and autonomy of the employee who is the perpetrator of the disciplinary offense;
- of the seriousness of the effects of the same by which is meant the level of risk to which the Companỳ reasonably maỳ have been exposed - pursuant to and for the purposes of Legislative Decree 231/2001 - as a result of the censured conduct;
- Of the other special circumstances accompanying the disciplinary offense.

Any disciplinary action taken will be communicated to the non-managerial employee, by LKIBS, by registered letter within 15 days of the expiration of the period given to the employee to submit his or her counter-arguments, as provided for in Article 227 of the relevant CCNL.

3.7.2 Sanctions for managerial employees

In the event of violation of the Model by employees, including those on secondment to LKIBS, with the status of executives, the Company, in the most serious cases, may resort to dismissal for just cause of the executive, to be prescribed in accordance with the provisions of the law and the collective agreement applied (National Collective Labor Agreement for executives of companies in the service, distribution and service industries).

3.7.3 Penalties for employees and consultants

In accordance with the provisions of Section 3.7.5, in the event of an established violation of the Model by a collaborator, LKIBS may consider such behavior to be contrary to the rules of fairness and thus the execution of the collaboration contract may be considered not in accordance with good faith, in violation of the provisions contained in Articles 1175 and 1375 of the Civil Code.

In the most serious cases, therefore, LKIBS may decide to terminate the collaboration contract. The termination of the contract is also provided for, a fortiori, if the conducts carried out in violation of the Model configure hypotheses of crime and as such are challenged by the Judicial Authority.

In the event of early termination of the contract, LKIBS will be obliged only to pay compensation for the work performed and expenses incurred up to the time of termination, subject to claiming damages if concrete damage to the Company results from the conduct.

3.7.4 Sanctions for members of corporate bodies

In the event of a violation of the prescriptions of the Model by the Administrative Body or its component, the same may be subject to evaluation by the Shareholders' Meeting which, if it detects in the violation a behavior that may lead to the revocation of the Director, or any requests to guarantee the rights, including financial, of the Company, shall provide for the adoption of the relevant measures.

In case of an ascertained violation of the Model by one or more Statutory Auditors, the Board of Statutory Auditors, with the abstention of the person involved, shall carry out the necessary investigations and, if necessary, inform the Administrative Body of LKIBS, which, in relation to the seriousness of the violation will convene the Shareholders' Meeting for the removal of the Statutory Auditor or other required measures.

3.7.5 Penalties for partners, suppliers and other third parties

The principles and contents of Model 231 are brought to the attention of all those with whom the Companỳ has contractual relations. Commitment to compliance with the law and the reference principles of Model 231 by third parties having contractual relations with LKIBS is provided for by a special clause in the relevant contract and is subject to acceptance by the third party contractor.

Any violation of the principles and requirements of the Model by partners, suppliers and other parties with whom LKIBS comes into contact is sanctioned in accordance with the provisions of the specific contractual clauses included in the relevant contracts.

LKIBS may, however, reserve the right to take all necessary measures if the behaviors integrating violations of the principles of behavior or the prescriptions set forth in Model 231 can also be configured with reference to the relationships in existence at the date of adoption of the Model and are contrary to the rules of fairness and good faith and therefore the execution of contracts is contrary to civil law canons, in violation of the provisions contained in Articles 1175 and 1375 of the Civil Code.

This is without prejudice to any claim for compensation should pecuniary or non-pecuniary damage to the Companỳ result from the conduct.

4. IDENTIFIED SENSITIVE ACTIVITIES AND RELATED SPECIAL REFERENCE PARTS

As explained in the General Section, the preparation (and subsequent updates) of this Model began with the identification of the activities carried out by the Company and the consequent identification of "sensitive" business activities potentially at risk of the commission of the offenses relevant under the Decree.

Below are the identified "sensitive activities" and the relevant Special Reference Parts in which each sensitive activity is regulated under this document.

Sensitive Activities	Special Part
1. Management of relations and obligations towards the public administration 2. Management of public funding	***A - Public Administration Relations Management***
3. Accounting management and preparation of financial statements and other corporate communications required by law 4. Management of relations with the Board of Statutory Auditors, the Auditing Firm and the shareholders 5. Tax compliance management 6. Management of intercompany relations 7. Corporate compliance management 8. Management of extraordinary operations	***B - Management of administrative, accounting and corporate activities.***
9. Cash management 10. Management of financial and treasury operations and relations with financial institutions	***C - Treasury management***
11. Recruitment and management of employees 12. Management of employee and contractor expense reimbursements	***D - Personnel Management***
13. Management of judicial and extrajudicial litigation	***E - Litigation management***
14. Management of gifts, donations and sponsorships	***F - Management of gifts, donations and sponsorships***
15. Procurement of goods and services, including professional and consulting appointments	***G - Purchasing Management***
16. Acquisition and management of job orders 17. Management of external communication activities	***H - Management of business and project activities***
18. Management and use of company and third-party information systems	***I - Information systems management***
19. Management of occupational health and safety compliance. 20. Environmental compliance management 21. Managing relationships with private certifying bodies	***L - Quality, occupational health and safety and environmental compliance management***

The Special Sections are aimed at defining, for each sensitive activity, the principles of behavior and the control garrisons to which all Recipients of the Model must adhere in order to prevent the commission of the offenses provided for in the Decree and ensure conditions of fairness and transparency in the conduct of business activities.

In particular, the following must be ensured:

- general control principals, applicable indiscriminately to all sensitive activities considered in the Special Parts and relating to:

  - Segregation of duties, between those who execute, authorize, account for and control a transaction;
  - Traceability and documentability of each transaction, including for the purpose of making *ex post* controls feasible
  - Assigned authorizing and signing authority consistent with assigned responsibilities and roles
  - Formalization and dissemination of corporate regulations defining the rules and operating methods to be followed in carrying out the activities under its responsibility
  - Implementation of a monitoring activity also aimed at keeping the control system updated;
- principles of conduct and control principals specific to each sensitive activity, regulated in each Special Section, which are complemented and declined, where applicable, in the relevant corporate regulations.

In addition, the Recipients shall, each for the aspects within his or her competence, adopt behaviors in accordance with the contents of the following documents:

- Code of Ethics;
- proxy system in place;
- Any other company documents, including company regulations, governing activities within the scope of the Decree.

It is also expressly forbidden to engage in conduct contrary to the provisions of current laws.

5. P.S. A - PUBLIC RELATIONS MANAGEMENT

The sensitive activities that the Company considers relevant in managing relations with the Public Administration are:

- Management of relations and obligations to the public administration (sec. 5.1);
- Management of public funding (sec. 5.2).

It should be noted that, Public Administration means public institutions, public officials and public service officers. Specifically:

- "Public institutions" means, by way of example and not limited to, state administrations (such as the Financial Administration, Guarantor and Supervisory Authorities, and Judicial Authorities), autonomous state companies and administrations, regions, provinces, municipalities, mountain communities, as well as their consortia and associations, university institutions, chambers of commerce, industry, handicrafts and agriculture, national, regional and local noneconomic public bodies, and administrations, companies and bodies of the national health service. A public function is also held by the Commission of the European Communities, the European Parliament, the Court of Justice and the Court of Auditors of the European Communities;
- "Public officials" means those who, whether public employees or private individuals, can or must form and manifest the will of the Public Administration, or exercise authoritative or certifying powers within the scope of a public law power. By way of example and not limitation, the following are considered public officials: officials of state administrations, regions, provinces, municipalities and their consortia and associations; representatives of Public Security Authorities, the Judicial Authority, the Guardia di Finanza, the Internal Revenue Service and other national non-economic public bodies; officials of the National Health Service; representatives of Supervisory and Supervisory Authorities; and officials of the Labor Inspectorate, INAIL and INPS;
- "Persons in charge of a public service" means those who, in any capacity, perform a public service, without being endowed with the typical powers of the public function, such as authoritative and certifying powers. By way of example but not limited to, employees or collaborators of Entities or Companies, whether public or private law, that perform public services, such as companies that are concessionaires or entrusted with public services, are considered public service appointees.

5.1. Management of relations and obligations towards the public administration

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Disclosure of company information or data to the public administration, including regulatory authorities • Institutional and representative relations, as well as relations of any kind with representatives of the Public Administration, including Supervisory Authorities • Relationships with public entities in the management of the activities under its responsibility (e.g., for administrative, social security, welfare, tax and health, occupational safety and environmental compliance and obligations or for obtaining authorizations, licenses and permits) • Inspections and audits by public officials or public service officers	• Administrative Body • Head of Business Unit • Human Capital • Administration and Personnel • Finance and Budget • RSPP	• Crimes against the Public Administration (Art. 24 and 25) - Fraud against the State or other Public Entity - Computer fraud against the State or other Public Entity - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence - (Conspiracy to) Embezzlement and Embezzlement by profiting from the error of others • Corporate crimes (Art. 25-ter) - Obstructing the exercise of the functions of public supervisory authorities

5.1.1. Principles of behavior specific

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Ensure that relations with the Public Administration during communications and fulfillments take place in full compliance with applicable laws and regulations;
- Comply with the current power of attorney system;
- Maintain fair, transparent, impartial and cooperative relations with public administration officials;
- provide, to its employees and collaborators adequate directives on how to conduct themselves in formal and informal contacts with public subjects;
- Diligently and promptly perform all duties required by applicable laws/regulations within the scope of its business;
- ensure that the documentation sent to or shared with the Public Administration, prepared both internally and with the support of collaborators/consultants, is complete, truthful and correct;
- submit documentation to individuals with appropriate powers, consistent with the proxy system in place, in order to verify, approve and sign it before forwarding it to the Public Administration;
- Promptly report any attempts by public officials to make improper requests;
- Ensure, in the case of inspection visits, that records are kept of the inspections received and their findings;
- Give full and immediate cooperation to public officials during inspections, providing the requested documentation and information in a timely and comprehensive manner.

It is also expressly forbidden:

- Corresponding, offering or promising, directly or indirectly, including in different forms of aid or contributions, payments or material benefits to public officials or public service officers or persons close to them, in order to influence their behavior and ensure advantages of any kind to the Company;
- Recognizing or promising money or other benefits to a third party, or to a person related to the latter, in order to generate undue advantages in favor of the Company thanks to the work of intermediation exercisable by the latter towards a public official or person in charge of a public service by virtue of existing (because public and notorious) or boasted relationships;
- Follow up on undue requests for money or other benefits from any person. In such cases, the employee must promptly inform his or her supervisor and suspend all relations with the requester;
- Yield to recommendations or pressure from public officials or public service officers;
- Hold misleading conduct toward the Public Administration such as to lead it into errors of judgment;
- Omit due information or submit untrue documents and statements in order to steer the decisions of the Public Administration in their favor;
- where the fulfillments are carried out using the Public Administration's computer/telematic system, alter the same and the data entered or improperly or illegally use the data processed, causing damage to the same Public Administration;
- omit to make, with due completeness, accuracy and timeliness, all the reports required by applicable laws and regulations to the Supervisory Authorities to which the company's business is subject, as well as the transmission of data and documents required by the regulations and/or specifically requested by the aforementioned Authorities;
- expose in the aforementioned communications and transmissions untrue data or information, or conceal/omit relevant facts that should have been disclosed;
- Engage in any behavior that is obstructive to the exercise of supervisory functions, including during inspection by the Supervisory Authorities.

5.1.2. Controls specific

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

The heads of the Organizational Units identified by corporate procedure PR14 "Information Flows and Attestations to the Supervisory Board" are also required to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the management of relations and fulfillments with the Public Administration.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Relations and fulfillments towards the Public Administration, including relations with public officials during inspection visits, may be managed exclusively by the Administrative Body and/or possibly by other Managers of Organizational Units formally authorized by the Administrative Body, taking into account the role and responsibilities assigned. In the event that relations and fulfillments are also managed by external collaborators and/or consultants, these must be granted the powers of representation on behalf of LKIBS by contract/letter of appointment/mandate and/or appropriate proxy.
- When transmitting applications, petitions, deeds, declarations or other documentation required by the Public Administration, the Heads of the Organizational Units responsible for the subject matter shall verify in advance the completeness, correctness and truthfulness of the documentation prepared by personnel (internal or external).
- Documentation to be sent to the Public Administration must be verified and signed by the Governing Body or other person with appropriate authority.
- Meetings with public officials must be attended by at least two corporate contacts.
- In the event of an inspection visit by public officials, the relevant person according to the specific type of visit who will attend and be available to officials throughout the visit must be notified immediately. If possible, at least two company contact persons should attend the visit.
- The minutes prepared by the public official following (or during) the visit must be signed by the Administrative Body or other person with appropriate authority who shall forward it to the Administrative Body for information.
- In the event that the inspector did not formalize any report, those who participated in the visit should prepare an internal report, including via *e-mail*, to be forwarded to their hierarchical contact person and the Administrative Body.
- Access to Public Administration computer/telematics systems should be allowed only to authorized personnel through assignment of personal *password-protected* users.
- All relevant documentation under this sensitive activity is archived by the relevant Organizational Units.

5.2. Management of public funding

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Preparation and transmission to relevant national or EU public bodies of documentation for obtaining funding • Management and reporting of disbursements • Management of relations with relevant national or community public bodies	• Administrative Body • Head of Business Unit • Administration and Personnel • Human Capital • Operational Control - Reporting	• Crimes against the Public Administration (Art. 24 and 25) - Aggravated fraud for obtaining public funds - Misappropriation of public funds - Misappropriation of public funds - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals

5.2.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must comply, insofar as applicable, with the principles of behavior defined for the sensitive activity "Management of relations and fulfillments towards the Public Administration," to which reference is made (Section 5.1).

It is also expressly forbidden:

- Allocate sums received from national or community public bodies as disbursements, contributions or financing for purposes other than those for which they were intended;
- Provide false or incomplete statements to the relevant bodies.

5.2.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the management of public financing.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Compliance related to public funding is coordinated by Administration and Personnel under the supervision of the Administrative Body.
- The documentation required for applying for public calls for funding is prepared, as far as technical aspects are concerned, by the staff of the Organizational Unit responsible for the subject matter (e.g., Human Capital with reference to funded training), with support, as far as administrative and economic-financial aspects are concerned, from Administration and Personnel.
- Additional documentation relating to the funding provided (e.g., reporting of amounts spent, etc.) may be forwarded to the appropriate body only after due verification (in terms of correctness and completeness) by the Head of the relevant Organizational Unit (including Operational Control - Reporting in the case of funding concerning research and development activities on contracts and Human Capital in the case of funding on training courses) and Administration and Personnel.
- The documentation submitted must be signed by the Administrative Body or other person with appropriate authority.
- Any audits by public inspectors on the reporting and use of funds granted must be handled in compliance with the control principals provided for inspection visits under the sensitive activity "Management of relations and compliance with the Public Administration" (referred to in Section 5.1.2).
- All relevant documentation under this sensitive activity is filed by Administration and Personnel.

6. P.S. B - MANAGEMENT OF ADMINISTRATIVE, ACCOUNTING AND CORPORATE ACTIVITIES

The sensitive activities that the Company considers relevant in the management of administrative, accounting and corporate activities are:

- Accounting management and preparation of financial statements and other corporate communications required by law (Sec. 6.1);
- Management of relations with the Board of Statutory Auditors, the Auditing Firm and shareholders (Section 6.2)
- Tax compliance management (sec. 6.3);
- Management of intercompany relations (sec. 6.4);
- Corporate compliance management (sec. 6.5);
- Management of extraordinary operations (sec. 6.6).

6.1. Accounting management and preparation of financial statements and other corporate communications required by law

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Management of the accounting system and chart of accounts • Management of accounting records and closing activities • Preparation and approval of the annual budget	• Administrative Body • Administration and Personnel • Finance and Budget	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - False corporate communications (including Misdemeanors) - Fictitious capital formation - Bribery among private individuals - Incitement to bribery among private individuals • Receiving, laundering and using money, goods or benefits of illicit origin, as well as self-money laundering (Article 25-octies) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration by other artifices - Concealment or destruction of accounting documents

6.1.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the rules and principles contained in the Civil Code, adopted accounting standards and other applicable laws and regulations;
- Comply with the current power of attorney system;
- Observe the rules of correct, complete and transparent accounting records in accordance with the criteria specified by the Law and the adopted accounting standards;
- Ensure timeliness, accuracy and compliance with the accrual principle in making accounting records;
- ensure that every transaction is not only properly recorded, but also authorized, verifiable, legitimate and consistent with the relevant documentation;

- comply with the criteria of reasonableness and prudence in the valuation and recording of accounting items, including valuation/estimation, keeping track of the valuation parameters and criteria that guided the determination of value;
- Ensure full traceability of the decision-making, authorization and control activities carried out in the process of closing accounts and preparing the financial statements;
- to behave correctly and transparently in all activities aimed at the preparation of the financial statements and other corporate communications, in order to provide shareholders and third parties with true and correct information on the Company's economic, asset and financial situation.

It is also expressly forbidden:

- represent in accounts - or transmit for preparation and representation in financial statements, reports and prospectuses or other corporate communications - false, deficient or, in any case, untrue data on the Company's economic, asset and financial situation;
- record transactions at incorrect values in the accounting records with respect to the underlying documentation, or against transactions that do not exist in whole or in part, or without adequate supporting documentation to allow for proper accounting and subsequently accurate reconstruction;
- Omit data and information required by current regulations or internal practices on the Company's economic, financial and asset situation;
- Putting in place activities and/or operations aimed at creating extra-accounting availabilities (e.g., through the use of invoices for non-existent transactions issued by third parties), or aimed at creating "slush funds" or "parallel accounting."
- Alter or destroy financial and accounting documents and information available in paper and/or electronic format.

6.1.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding accounting and financial statement aspects.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- The activities are managed, as far as accounting is concerned, by Administration and Personnel and, as far as budget preparation is concerned, by Finance and Budget, under the coordination of the Administrative Body and with the support of external consultants specialized in the field.
- Accounting records are made by Administration and Personnel through the dedicated application that allows access only to authorized personnel through personal *User ID* and *Password* (based on the tasks performed) and ensures that all transactions (and who performed them) are traceable and automatic checks are performed.
- Needs to change the access profiles of the dedicated application as well as the accounts in the chart of accounts must be approved by the Administrative Body, upon the possible proposal of the Administration and Personnel Manager.
- Administration and Personnel periodically conducts a review of application access profiles and chart of accounts.
- Accounting entries must be made by Administration and Personnel in accordance with adopted accounting principles, against verification of appropriate supporting documentation (e.g., invoices, contracts, etc.).

- There is a closing schedule monitored by the Administration and Personnel Manager through confirmation of completion of planned activities.
- At the time of closing the financial statements, Finance and Budget performs, in coordination with external consultants, the adjustment/closing entries that must be verified and approved by the Head of Finance and Budget. It is also responsible for the interaction between the various structures involved, the statutory auditors and the Board of Auditors.
- The Finance and Budget Manager conducts an analysis of financial statement items characterized by a high valuation component, or by specific complexity factors related to the application of accounting standards, or non-recurring. The analysis must be shared with the Administrative Body.
- The final system-extracted audit balance sheet is subjected to balancing and verification by Finance and Budget, which, in particular, performs a comparative analysis of the income statement and balance sheet balances (including against the previous year's final balance sheet and the current year's *budget/forecast*) in order to identify possible anomalies. The Finance and Budget Manager conducts a *review* of the analysis performed.
- The draft periodic financial statements, financial statement schedules, notes to the financial statements, and management report are prepared by Finance and Budget with the help of the information application, checked by the Finance and Budget Manager, and approved by the Administrative Body.
- The financial statements must be forwarded to the Auditing Company in order to enable it to carry out the checks preparatory to the issuance of the financial statement certification.
- The budget, approved by the Governing Body, must be submitted to the General Meeting of Shareholders for approval in accordance with the provisions of the Civil Code.
- Supporting documentation to the accounting records and financial statements as well as the audits and analyses performed must be filed, by jurisdiction by Administration and Personnel and Finance and Budget.

6.2. Management of relations with the Board of Statutory Auditors, the Auditing Firm and the shareholders

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Retention and disclosure of data and information subject to audit by shareholders, auditors, and auditing firms • Managing relationships with shareholders, auditors, and auditors during related audits	• Administrative Body • Administration and Personnel • Finance and Budget	• Corporate crimes (Art. 25-ter) - Prevented control - Bribery among private individuals - Incitement to bribery among private individuals

6.2.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the current power of attorney system;
- to maintain, with respect to the control activity attributed to the Members, Auditors and Auditors, a correct, transparent and cooperative behavior such as to enable them to carry out their institutional activities;
- Provide Members, Auditors and Auditors with free and timely access to requested data and information;
- Provide Members, Auditors and Auditors with accurate, complete, faithful and truthful information.

It is also expressly forbidden:

- Engaging in conduct that hinders the performance of control activities by Shareholders, Auditors and Auditors by concealing required documents and information, or by providing incomplete, unclear or misleading documents and information.
- Pay or offer, directly or indirectly, including in different forms of aid or contributions, payments or material benefits to the counterparty or persons close to them, in order to influence their behavior and ensure advantages of any kind to the Company.

6.2.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

The heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" are also obliged to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the management of relations with Shareholders, Statutory Auditors and Auditors.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Relations with Members, Statutory Auditors, and Auditors are maintained exclusively by the Governing Body, Administration and Personnel, and Finance and Budget, which assist the auditing bodies in the course of audits and fulfill related information requests.
- All documentation delivered to the Members, Auditors and Auditors must first be verified for completeness and correctness by the Administration and Personnel Manager and the Finance and Budget Manager, according to their respective responsibilities.
- Relevant communications to Auditors and Auditors must be done formally (via e-mail) and be traceable.
- You must keep track of all documentation delivered (e.g., by emailing it and/or requesting an email confirmation of receipt).
- Relevant meetings with auditors and auditors must be attended by at least two expressly authorized corporate contacts.
- All relevant documentation under this sensitive activity is filed by Administration and Personnel and Finance and Budget, according to their respective responsibilities.

6.3. Tax compliance management

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Calculation and settlement of taxes (direct, indirect, etc.) • Preparation and submission of tax returns • Management of relations with the Internal Revenue Service	• Administrative Body • Administration and Personnel	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, and self-money laundering (Article 25-octies) - Self-money laundering • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration through the use of invoices or other documents for nonexistent transactions - Fraudulent declaration by other artifices - Unfaithful declaration - Failure to declare - Issuance of invoices or other documents for nonexistent transactions

		- Concealment or destruction of accounting documents - Undue compensation

6.3.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the current power of attorney system;
- Ensure monitoring of tax deadlines and tax news;
- submit tax returns, as well as arrange for the making of related payments, in accordance with the provisions and timelines set forth in the relevant laws and regulations;
- disclose, in tax returns, assets and liabilities in a truthful and transparent manner in order to enable the competent Authorities to correctly reconstruct the Company's income or turnover;
- Pay the amounts of tax due, using only eligible and existing credits as offsets;
- Ensure the traceability of the process related to the transmission of tax returns to the relevant Authorities, to be carried out in accordance with the laws and regulations.

It is also expressly forbidden:

- make use of invoices or other documents for nonexistent transactions and record them in the mandatory accounting records, indicating such fictitious taxable items in one of the tax returns;
- Carry out simulated transactions objectively or subjectively or make use of false documents or other fraudulent means suitable for hindering the assessment and misleading the Tax Administration, indicating in one of the tax returns asset items for an amount lower than the actual amount or fictitious liability items or fictitious credits and deductions, in order to evade income tax or value-added tax;
- Prepare and send tax returns to the competent authorities containing false, fabricated, incomplete or otherwise untrue data;
- Omit tax returns/communications, which are required by law, in order to evade taxes;
- take advantage of special tax regimes or exemptions and deductions in the knowledge of the absence of the regulatory prerequisites (subjective and objective), through altering accounting documents or concealing the underlying factual conditions;
- Simulately alienate or perform other fraudulent acts on the Company's assets suitable for rendering ineffective, in whole or in part, any compulsory collection procedure by the Tax Administration;
- Use undue or nonexistent credits in compensation;
- Issue invoices or issue other documents for non-existent transactions in order to enable third parties to evade income or value-added taxes;
- Alter, conceal, or destroy all or part of financial and accounting documents and information available in paper and/or electronic form that are required to be retained.

With reference to the management of relations and fulfillments towards the Tax Administration, the principles of conduct defined for the sensitive activity "Management of relations and fulfillments towards the Public Administration," to which reference is made (Section 5.1), must also be complied with insofar as applicable.

6.3.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board," there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding tax compliance and relations with the Internal Revenue Service.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Tax compliance is handled by Administration and Personnel and Finance and Budget, with the support of external consultants specializing in the field and under the coordination of the Administrative Body.
- Monitoring of tax deadlines and tax news is carried out by outside consultants.
- Administration and Personnel extracts and transmits to external consultants, subject to verification by its Manager, the data necessary to calculate direct taxes.
- The external consultant calculates direct taxes and prepares the Company's IRES and IRAP returns.
- Administration and Personnel performs a consistency check of the amounts of direct taxes to be settled by the Company, compared with the amounts set aside in the budget, as well as an analysis of the variances between the IRES and IRAP Returns prepared and those of the previous year.
- External consultants process data on VAT taxable income, provided by Administration and staff, and, on the basis of the due dates, prepare the Annual VAT Data Report and the Annual VAT Return.
- Calculations related to withholding taxes for self-employed and salaried income as withholding agent are carried out by Administration and Personnel and forwarded, after verification by its Manager, to the external consultant who prepares Form 770 and Single Certificates.
- The external consultant provides for the telematic submission of the Declaration and Disclosure Forms, subject to verification by Administration and Personnel (and, with reference to direct taxes, by the auditing firm) and signature by a person with appropriate powers (and, with reference to direct taxes, by the Representative of the auditing firm who signs the audit report).
- Following successful transmission, the external consultant sends the Company a copy of the transmitted Declaration Forms and a receipt of receipt from the Internal Revenue Service.
- Tax payments are made by Administration and Personnel, subject to the approval of the Administrative Body, within the deadlines set for tax settlement.
- All relevant documentation under this sensitive activity is filed by Administration and Personnel and the external consultant.

With reference to the management of relations and fulfillments towards the Tax Administration, the control principals defined for the sensitive activity "Management of relations and fulfillments towards the Public Administration," to which reference is made (Section 5.1), must also be complied with insofar as applicable.

6.4. Management of intercompany relations

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Underwriting and execution of intercompany contracts • Management of related reports	• Administrative Body • Head of Business Unit • Compliance and Quality • Administration and Personnel	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - (Conspiracy to) Improper return of contributions - Bribery among private individuals - Incitement to bribery among private individuals • Receiving, Laundering and Use of Money, Goods or Benefits of Unlawful Origin, and Self-Money Laundering (Article 25-octies Decree) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration through the use of invoices or other documents for nonexistent transactions - Fraudulent declaration by other artifices - Unfaithful declaration - Issuance of invoices or other documents for nonexistent transactions - Fraudulent evasion of tax payment

6.4.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the power of attorney system in place;
- Ensure that all intercompany transactions are conducted fairly, in deference to existing service contracts, and that fees are in line with those provided by the market for similar goods/services.

It is also expressly forbidden:

- Approve contracts/orders/invoices against intercompany transactions, in whole or in part fictitious and/or unnecessary and/or at prices not aligned with market prices;
- Define, with regard to intercompany loans, repayment terms that are not in line with market values.

6.4.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

The heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" are also obliged to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding intercompany relations.

In addition, as it relates to the sensitive activity in question, the following procedure adopted by the Company is applied to supplement the reported control safeguards:

- PR04 "Project Management," with particular reference to the parts of the procedure dealing with the management of intercompany billing.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Intragroup operations are coordinated by the Administrative Body, with support from Compliance and Quality and Administration and Personnel.
- Intragroup relations must be regulated through contracts that clearly regulate the roles and responsibilities of the counterparties involved as well as the services rendered and the methods for determining the fees expected based on a comparative analysis with the market and any *transfer pricing* rules defined by the Administrative Body.
- Intragroup contracts must be signed by individuals with appropriate powers consistent with the current power of attorney system.
- Administration and Personnel must perform *intercompany* reconciliations periodically to ensure proper recording in the relevant accounting period.
- All relevant documentation under this sensitive activity is archived by Compliance and Quality and Administration and Personnel.

6.5. Corporate compliance management

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Resolutions regarding contributions • Resolutions involving profits and reserves • Resolutions regarding actions • Resolutions regarding the reduction of share capital or inherent in mergers with another company or demergers • Capital transactions • Managing relations with the assembly in the person of members	• Administrative Body • Finance and Budget	• Corporate crimes (Art. 25-ter) - Transactions to the detriment of creditors - Improper return of contributions - Illegal distribution of profits and reserves - Unlawful transactions in the company's or the parent company's stock or shares - Unlawful influence on the Assembly - Fictitious capital formation

6.5.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the power of attorney system in place;
- Ensure that all types of corporate transactions are conducted by the Company in full compliance with applicable laws and regulations;
- Observe all legal regulations to protect the integrity and effectiveness of share capital, so as not to harm the guarantees of creditors and third parties in general;
- Ensuring the smooth operation of the Company and the Corporate Bodies, guaranteeing and facilitating all forms of internal control over corporate management;
- Ensure the free and proper formation of the will of the assembly.

It is also expressly forbidden:

- return contributions to shareholders or release them from the obligation to make them, outside the cases of legitimate reduction of share capital provided by law;
- Distribute profits or advances on profits not actually earned or allocated by law to reserves;
- Allocate reserves in cases where this is not permitted by law;
- Purchase or subscribe for shares of the Company and/or its subsidiaries outside the cases provided for by law, with injury to the integrity of the share capital;
- proceed in any way to fictitious formation or increase of share capital or carry out reductions of share capital, mergers or demergers in violation of legal provisions protecting creditors;

- determine or influence the passing of resolutions at the shareholders' meeting by engaging in simulated or fraudulent acts aimed at altering the regular process of forming the will of the shareholders' meeting.

6.5.2. Specific control measures

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information Flows and Attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding corporate obligations.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Corporate compliance is handled exclusively by the Governing Body with the support of Finance and Budget and any specialized outside professionals who:
  - verify compliance with the statutory and regulatory provisions applicable to the functioning of the Administrative Body and the Assembly;
  - shall convene the Shareholders' Meeting in the manner and within the time limits prescribed by applicable law;
  - ensure that the resolutions passed comply with all applicable laws and regulations;
  - take minutes of meetings on the company's books, making them fully accessible to the supervisory bodies;
  - shall place on file, archive and preserve in accordance with the law the convocations, resolutions, minutes and all other relevant documentation.
- All relevant documentation under this sensitive activity is filed by Finance and Budget.

6.6. Management of extraordinary operations

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Merger transactions with other company • Acquisition of shareholdings • Splits	• Administrative Body • Finance and Budget	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Transactions to the detriment of creditors - Bribery among private individuals - Incitement to bribery among private individuals • Receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, and self-money laundering (Article 25-octies) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater) and Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy - Associations for the purpose of terrorism, including international terrorism or subversion of democratic order • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration by other artifices - Fraudulent evasion of tax payment

6.6.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Ensure that all kinds of extraordinary transactions are conducted by the Company in full compliance with applicable laws and regulations;
- Comply with the power of attorney system in place;
- Observe all legal regulations to protect the integrity and effectiveness of share capital, so as not to harm the guarantees of creditors and third parties in general;
- check in advance the available information on the companies that constitute the contractual counterparty in the extraordinary transaction in order to establish relationships only with individuals whose identity is certain (including any individuals on whose behalf they are acting), who must prove with documentation the existence of appropriate powers of representation of the contractual counterparty and their engagement exclusively in lawful activities;
- ensure that every extraordinary transaction is not only recorded in accordance with legal requirements, but also legitimate, authorized and verifiable;
- proceed to the valuation and recording of economic and financial elements related to extraordinary transactions in accordance with the criteria of reasonableness and prudence, clearly illustrating in the relevant documentation the criteria that guided the determination of the value of the extraordinary transaction;
- behave correctly, transparently and cooperatively in all activities aimed at preparing prospectuses and other corporate communications aimed at an extraordinary transaction, in order to provide shareholders and third parties with true and fair information on the economic and financial situation of the Company and the transaction itself.

It is also expressly forbidden:

- Carry out extraordinary transactions in violation of legal provisions to protect creditors;

- Establish relationships or carry out extraordinary transactions with counterparties if there is a well-founded suspicion that this may expose the Company to the risk of committing (including concurrently) criminal conspiracy, receiving, money laundering, or the use of money, goods or utilities of illicit origin, as well as self-money laundering;
- Conducting activities related to the management of extraordinary transactions in an "abnormal" manner, employing, substituting or transferring financial assets from crime, so as to hinder the identification of their criminal origin;
- requesting or inducing representatives of the counterparties involved in the process in question (e.g., counterparty representatives, external *advisors*, etc.) to recognize or promise money or other benefits, for themselves, third parties or for the benefit of the Company, as the price of their illicit mediation with a public official or a person in charge of a public service or as remuneration in connection with the exercise of their functions or powers.

6.6.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information Flows and Attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding extraordinary transactions.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Extraordinary transactions are handled exclusively by the Administrative Body with the support of Finance and Budget and any specialized outside professionals.
- Any extraordinary transactions must be submitted to the Assembly for prior deliberation.
- Prior to each extraordinary operation, a preliminary assessment must be carried out and formalized by the Administrative and Finance and Budget Body, with the possible support of a specialized external advisor, aimed at verifying its appropriateness, feasibility and strategic coherence with respect to the Group's objectives as well as in order to decide whether to carry out *due diligence* (legal, fiscal, accounting, etc.), also with the support of specialized external *advisors.*
- With regard to counterparties that are not widely recognized in the market and in accordance with the criteria of reasonableness and proportionality, a review aimed at assessing the integrity and identifying potential reputational risks of the counterparty should also be carried out.
- Relevant documentation produced as part of the *due diligence* and, in general, of the transaction must be verified, where deemed necessary, by outside attorneys/tax advisors.
- All extraordinary corporate transactions and related binding agreements must be signed by individuals with appropriate powers.
- Documentation of the transaction (presentations, financial statements, results of *due diligence,* etc.) must be explained to the Assembly.
- All relevant documentation under this sensitive activity is filed by Finance and Budget.

7. P.S. C - TREASURY MANAGEMENT

The sensitive activities that the Company considers relevant in treasury management are:

- Cash management (sec. 7.1);
- Management of financial and treasury operations and relations with financial institutions (sec. 7.2).

7.1. Cash management

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Use of the cash box • Cash reconciliations	• Administrative Body • Administration and Personnel • Office Coordinator	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals

7.1.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Operate in compliance with current regulations on payment instruments, traceability of financial flows and anti-money laundering;
- Comply with the power of attorney system in place;
- Use cash on hand appropriately, within the limits of business needs and in any case for amounts of moderate value;
- Always keep the cash fund inside the safe where excessive amounts of money should never be stored.

It is also expressly forbidden:

- Pay or offer/promise payments or material benefits or gifts of money or other utility to public officials or public service officers or private counterparts or persons close to them to secure advantages of any kind to the Company;
- Follow up on undue requests for money or other benefits from any person. In such cases, the employee or collaborator must promptly inform his or her superior and suspend all business relations with the requester;
- Use cash as a means of payment and collection outside of expressly permitted cases or otherwise improperly. The use of cash should be reduced to an absolute minimum and the banking channel should be used preferentially in making payment transactions;
- Accept cash receipts for amounts that are in the aggregate equal to or greater than the reference threshold specified by current regulations;
- Transfer cash or bearer bank or postal passbooks or bearer securities in euros or foreign currencies, when the value of the transaction, including fractional transactions, is in the aggregate equal to or greater than the threshold specified by current regulations;
- Make cash payments that are not properly documented and authorized;
- re-introduce into the monetary circuit counterfeit banknotes or coins, or even simply suspected counterfeits. Such banknotes must be retained and handed over to a credit institution.

7.1.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding cash management.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- The cash fund is managed by the Office Coordinator under the supervision of the Administrative Body.
- Amounts in cash shall not exceed the maximum amount limit stipulated by the applicable regulations on cash transfers.
- All payments through petty cash must be authorized, upon reasoned request, by the responsible manager as well as recorded and documented by the relevant receipts that must be kept.
- On a monthly basis, Administration and Personnel with the support of the Office Coordinator performs the reconciliation of the cash balance (in order to verify the alignment between the physical balance and the accounting balance), keeping track of the checks performed and filing the related documentation. The Administration and Personnel Manager approves the checks performed.
- Replenishment of petty cash must be authorized consistent with the current system of powers.
- All relevant documentation under this sensitive activity is filed by Administration and Personnel.

7.2. Management of financial and treasury operations and relations with financial institutions

Related activities (illustrative)	**Main Contacts/Organizational Units Involved.**	**Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)**
• Managing relationships with financial institutions when opening/igniting, modifying and closing current accounts, loans, guarantees and surety bonds • Management of payments and collections • Accounts receivable and overdue management	• Administrative Body • Administration and Personnel • Finance and Budget • Head of Business Unit	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Receiving stolen goods, money laundering and use of money, goods or utilities of unlawful origin, and self-money laundering (Article 25-octies) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration through the use of invoices or other documents for nonexistent transactions - Fraudulent declaration by other artifices - Concealment or destruction of accounting documents - Fraudulent evasion of tax payment • Offenses involving non-cash payment instruments (Article 25-octies.1) - Computer fraud that produces transfer of money, monetary value, or virtual currency - Misuse and forgery of non-cash payment instruments • Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater) and Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy - Associations for the purpose of terrorism, including international terrorism or subversion of democratic order

7.2.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Operate in compliance with current regulations on collection and payment instruments, traceability of financial flows and anti-money laundering;
- Comply with the current proxy system;
- preferentially use the banking channel and exclusively licensed financial operators in making collections and payments, funds transfer, employment or other use of financial assets;
- Use the non-transferability clause for any bank check transactions;
- Arrange congruous payments with underlying documentation (e.g., authorized invoice) and to the bank account reported by the supplier;
- Immediately report any attempt to falsify and misuse non-cash payment instruments;
- Ensure that loans are entered into with leading bank counterparties or other qualified lenders.

It is also expressly forbidden:

- Pay or offer/promise payments or material benefits or gifts of money or other utility to public officials or public service officers or private counterparts or persons close to them to secure advantages of any kind to the Company;
- Follow up on undue requests for money or other benefits from any person. In such cases, the employee or collaborator must promptly inform his or her superior and suspend all business relations with the requester;
- Make payments that are not adequately documented and authorized and/or in countries other than the country where the counterparty resides or where the *business/commercial* service is performed;
- Arrange payments or collect money to/from countries on major international *blacklists.*
- Approve invoices payable against simulated or non-existent services in whole or in part;
- open accounts or savings accounts anonymously or in fictitious names and use those that may have been opened in foreign countries, where this is not related to legitimate economic activity;
- Issue bank or postal checks that do not bear the name or company name of the payee and the non-transferability clause;
- Make transfers, including international transfers, without explicit indication of the counterparty;
- Managing financial resources, including intra-group, in an "abnormal" manner, employing, substituting or transferring financial assets of illicit origin, so as to hinder the identification of their criminal origin;
- Carry out transactions suitable for facilitating the laundering of money from illegal or criminal activities;
- engage in "off-market" financial transactions, i.e., on terms that differ substantially from those prevailing in the market at the time the transaction is entered into;
- Misuse (and/or encourage the misuse by third parties) of credit/debit cards of which one is not the holder, or any other similar document that enables the withdrawal of cash or the purchase of goods or the provision of services, or in any case any other payment instrument other than cash;
- Forging or altering non-cash payment instruments;
- Abusively entering, directly or through an intermediary, a computer or telecommunications system protected by security measures against the will of the holder of the right of access, including for the purpose of misusing, falsifying or altering non-cash payment instruments.
- Use/access computer equipment, devices or programs suitable for committing crimes involving non-cash payment instruments (e.g., acquiring the digital identity and payment data of third parties).

7.2.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by Corporate Procedure PR14 "Information Flows and Attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding financial transactions.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Financial and treasury operations and relations with financial institutions are managed, according to their respective responsibilities, by Finance and Budget and Administration and Personnel under the coordination of the Administrative Body.

Managing relationships with financial institutions when opening/igniting, modifying and closing current accounts, loans, guarantees and surety bonds

- The Finance and Budget Manager is responsible, in agreement with the Administrative Body, for negotiating economic and contractual conditions with financial institutions, selecting those whose conditions applied are most advantageous.
- At least two formally authorized corporate contacts participate in negotiations with financial institutions.
- Operations to open, change and close current accounts and to take out, change and extinguish loans, guarantees and surety bonds are authorized in advance by the Administrative Body and the related contracts are signed by individuals with appropriate powers.
- All relevant documentation is filed by Administration and Personnel.

Management of payments and collections

- Treasury operations must be handled by a formally authorized Administration and Personnel contact person who cannot record invoices or manage the supplier registry, under the supervision of the Administration and Personnel Manager.
- All banking transactions must be handled through the treasury information system and *remote* banking system structured on the basis of specific authorization profiles.
- Access to the *remote banking* system with "device" or "viewing" profile must be differentiated according to the role held and duties performed. In particular, access with "device" profile is allowed only to individuals with appropriate powers.
- Payments are arranged only to the bank accounts indicated by the supplier at the time of contracting or subsequently through written communications from the supplier. In the event of a supplier's request for a change in bank account details, the Administration and Personnel Manager shall make the appropriate preventive checks (e.g., by contacting the supplier's contact person by telephone) and file documentary evidence to substantiate the change.
- Before proceeding to payment Administration and Personnel verifies, through system functionality, that there is *3-way* match between order, goods/services entry and recorded invoice. If there is a mismatch, invoices are blocked and cannot be processed for payment until the anomaly is resolved.
- Periodically, Administration and Personnel selects, in accordance with Finance and Budget, which is in charge of financial planning, the payments to be made (pre-approved by the relevant order managers), automatically generating the payment proposal on the system, which is uploaded to the bank's *remote banking,* thus generating the payment bill and closing the accounts payable.
- Before making the payment proposal on the *remote banking* system, Administration and Personnel checks that the data for transfers always show clear identification of the counterparty (i.e., that it is not possible to make payments to so-called encrypted accounts).
- Any manual transfers must be verified in advance by the Administration and Personnel Manager and authorized by the Administrative Body.

- Checks are implemented to ensure that there is always a match between the person receiving the transfer and the supplier/collaborator to be paid, as well as between the bank account used for the transfer and the one entered in the supplier master data and/or in the supporting documentation (contract, notice of change of bank account, etc.).
- Periodically, Administration and Personnel reconciles payments and collections made through the *remote banking* system.
- On a monthly basis, Administration and Personnel performs bank reconciliations that are subsequently verified by the Administration and Personnel Manager.
- Administration and Personnel must ensure the accuracy and completeness of all accounting records related to cash receipts received, as compared to what is in the available supporting documentation and matching them to the relevant credit items.

Accounts receivable and overdue management

- Finance and Budget performs credit monitoring and activates the relevant Head of Business Units to manage overdue and related reminders.
- Any repayment plans with respect to overdue receivables are defined and agreed with customers by the relevant Head of Business Unit after sharing with the Administrative Body.
- In the event that reminders end in failure and repayment plans are not agreed upon with customers, the relevant litigation must be opened with the support of external reference attorneys and in compliance with the control principals defined in Section 9.1 "Management of judicial and extrajudicial litigation" below.
- The Finance and Budget Manager approves the write-down and possible write-off of overdue receivables in agreement with the Administrative Body and only if adequately justified. In the case of write-off of receivables, an external legal opinion is also sought where appropriate.
- All relevant documentation is filed by Finance and Budget and the relevant Head of Business Units.

8. P.S. D - PERSONNEL MANAGEMENT

The sensitive activities that the Company considers relevant in personnel management are:

- Recruitment and management of employees (sec. 8.1);
- Management of employee and contractor expense reimbursement (sec. 8.2).

8.1. Recruitment and management of employees

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Selection and recruitment of new employees • Management of employee incentive and development policies • Administrative management of employee personnel, including the management of relations with public entities with reference to social security and welfare obligations and personnel belonging to protected categories or whose employment is facilitated	• Administrative Body • Head of Business Unit • Human Capital • Administration and Personnel	• Crimes against the Public Administration (Art. 24 and 25) - Fraud against the State or other Public Entity - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence - (Conspiracy to) Embezzlement and Embezzlement by profiting from the error of others • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Crimes against the individual (Art. 25-quinquies) - Illicit intermediation and labor exploitation • Crime of employment of third-country nationals whose stay is irregular (Art. 25-duodecies) • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration by other artifices

8.1.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- comply with applicable labor laws and regulations (e.g., on minimum wages, social security and welfare contributions, residence permits, protected categories, etc.);
- Ensure working conditions that respect personal dignity, equal opportunities, and a suitable working environment;
- Comply with the power of attorney system in place;
- operate, when hiring, promoting and incentivizing employees, in accordance with the meritocracy criterion and taking into account the real needs of the Company;
- check available information on candidates in advance in order to establish relationships only with individuals who enjoy a good reputation, who are engaged only in lawful activities and whose ethical culture is comparable to that of the Company;
- carry out selection and recruitment activities exclusively on the basis of assessments of technical, ethical and aptitude suitability; the activity must be guided by criteria of transparency in the assessment of the requirements of competence and professionalism, individual ability and potential;
- ensure that the definition of economic conditions, both at the time of hiring and at the time of career advancement and the recognition of *benefits* and *bonuses* is consistent with the position held in the company and the responsibilities/tasks assigned;

- To ensure that the obligatory fulfillments required when hiring personnel (including those belonging to protected categories), as well as in connection with the administrative management of the same, are handled with the utmost diligence and professionalism, so as to provide clear, accurate, complete, faithful and truthful information;
- Ensure that relations with Public Officials related to personnel management are marked by maximum transparency, cooperation, helpfulness and in full respect of the institutional role.

It is also expressly forbidden:

- operate according to the logic of favoritism;
- discriminate against workers because of race, gender, sexual orientation, social and personal position, physical and health condition, disability, age, nationality, religion or political and/or personal beliefs;
- Promising or granting promises of employment as a quid pro quo for activities contrary to laws and internal rules and regulations;
- select or promise to select employees who are close to or suggested by public officials or any private third party, or pay or promise to pay them compensation in excess of what is due or market rate, in order to secure advantages of any kind for the Company;
- enter, in the personnel records, fictitious employees, including for the purpose of creating extra-accounting availabilities or to obtain benefits of any kind;
- Hiring workers who are not of working age or foreign workers without residence permits, or whose permits have expired (and for which renewal has not been applied for), been revoked or cancelled;
- Displaying untrue facts in the documentation sent to or shared with the Public Administration when hiring and managing employees, or concealing relevant facts;
- Promising or recognizing *benefits*, *bonuses*, career advancement or salary increases as a quid pro quo for activities that are contrary to laws and internal rules and regulations;
- Promising or granting *benefits*, *bonuses*, career advancement or salary increases to resources close to or liked by public officials or any private third party with whom the Company deals when this is not in accordance with the real needs of the company and does not respect the principle of meritocracy.

With reference to the management of relations and fulfillments towards public subjects, the principles of conduct defined for the sensitive activity "Management of relations and fulfillments towards the Public Administration," to which reference is made (Section 5.1), must also be complied with insofar as applicable.

8.1.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board," there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding personnel management.

In addition, as they are related to the sensitive activity in question, the following procedures/rules adopted by the Company are applied to supplement the reported control safeguards:

- Human capital management operations manual;
- PR07 "Timesheet/ CV Update/ Address Book," with particular reference to the part of the procedure concerning *timesheet* accounting on projects of hours worked.
- PR15 "Compliance with the requirements of social responsibility according to the SA8000 standard and gender equality according to UNI/PdR 125:2022 practice - Management of reports and complaints."

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

Selection and recruitment of new employees

- The process of selecting and hiring new staff is managed by Human Capital under the coordination of the Administrative Body.
- In the event of a staffing requirement, the Head of Business Unit (if the requirement concerned a job order) or other concerned Head of Organizational Unit (if it concerned, for example, location requirements) sends by *e-mail* to Human Capital the request, which must contain the necessary information for the selection, including: type and reason for the request, type of contract and classification, possible duration, and job description.
- Requests for new personnel must be authorized by the Human Capital Manager and the Administrative Body.
- The selection can be handled internally or with the support of recruiting/head *hunter* companies. In the second case, a special clause must be included in the contracts/letters of engagement entered into, whereby the counterparty declares that it has received and understood the LKIBS Model 231 (including its annexes) and that it undertakes to adhere to and abide by the principles contained therein.
- Human Capital conducts a review and skimming of the collected *resumes in* order to define the shortlist of candidates to be contacted.
- At least two interviews aimed at assessing the i) psycho-aptitude (by Human Capital) and ii) technical characteristics of the candidates (by the Head of the requesting Organizational Unit or, in the case of a search for an apical position, by the Administrative Body) must be conducted during the selection process. The results of the interviews must be formalized, giving reasons, in particular, for the final choice made.
- Once the selection phase is completed, Human Capital formulates the economic proposal to be presented to the candidate, which is verified in advance by the Human Capital Manager and approved by the Administrative Body, also in order to ensure that the economic conditions are consistent with market levels, company policies, the position held by the candidate and the responsibilities/duties assigned.
- If the proposal is accepted, Human Capital must require the candidate to submit the necessary documentation for the purpose of employment (e.g., ID, social security number, self-certification of educational qualification and professional qualifications/registration, etc.).
- As part of the pre-employment checks, the candidate should be asked to state:
  - the possible existence of potential conflicts of interest (e.g., holding or having held public office or having been a member of public bodies) and/or relationships of spouse, kinship or affinity with members of the Public Administration;
  - The existence of any pending criminal proceedings/charges against them.
- Human Capital must verify, if the selection and hiring process involves workers from non-EU countries, that the candidate has valid residence documents.
- Hiring contracts must be submitted for approval and signature of person with appropriate authority.
- Human Capital must ensure that employment contracts include the required clause of compliance with Legislative Decree 231/2001 and adherence to Model 231 (and its annexes) made available to newly hired employees on the company dashboard and that they participate in the mandatory 231 training course on an *online* platform.
- All relevant documentation as part of the recruitment and selection process is archived by Human Capital.

Management of employee incentive and development policies

- Personnel incentive and development policies are managed by Human Capital under the coordination of the Governing Body.
- The Head of Human Capital ensures the management of a formalized and structured process of periodic employee evaluation related to employees' personal development plans to support career

advancement, merit increases, *bonuses* and performance awards. This process must be approved in advance by the Administrative Body.

- Recognition of career advancement, merit increases, *bonuses* and awards must be approved by the Administrative Body and the Head of Human Capital, also upon the proposal of the Head of the relevant Organizational Unit.
- These measures must be formalized in special letters prepared by Human Capital and approved by a person with appropriate authority.
- All relevant documentation as part of the process of managing personnel incentive and development policies is archived by Human Capital.

Administrative management of employee personnel

- Personnel administrative aspects are handled by Human Capital and Administration and Personnel with the support of an employment consultant.
- Access to personnel records in the current information system should be allowed only to the appropriate individuals.
- Human Capital carries out, periodically, a systematic review of the personnel registry.
- Any entry or change in employee records must be tracked and supported by documentation proving the start, change, or termination of employment.
- Employee attendance is recorded by means of *timesheets* duly filled in by each employee on the company dashboard and approved by the relevant manager.
- Vacations, leave and overtime must be authorized in the system by the Manager of the employee concerned.
- Based on the shared schedule and the data recorded on the management system, the Labor Consultant processes payroll coupons and F24 Forms for the payment of contributions and withholding taxes, making all necessary verifications.
- Administration and Personnel, upon receiving the draft coupons and F24 Forms, makes the necessary verifications and notifies the Labor Consultant of any changes and/or errors via *e-mail*.
- The Labor Consultant sends the coupons and the statement with the contributions to be paid to Administration and Personnel, which processes the payments, subject to verification by the Head of Administration and Personnel and in compliance with the control safeguards provided for the sensitive activity "Management of financial and treasury operations and relations with financial institutions," to which reference is made (Section 7.2).
- Human Capital ensures periodic monitoring of the regularity of residence permits/residence cards of foreign workers. In case of expiration, it requires the employee, with adequate advance notice, to arrange for the renewal of permits, unless it is impossible to continue the employment relationship.
- In relation to personnel belonging to protected categories, Human Capital verifies, with the support of the Labor Consultant, any overdrafts, monitoring compliance with legal requirements and thresholds in order to determine any needs.
- All documentation required by *law* is verified by Administration and Personnel and the Labor Consultant and forwarded to the appropriate agencies (INAIL, INPS, etc.) *online* by the Labor Consultant.
- All relevant documentation within the administrative personnel management process is filed by Human Capital and Administration and Personnel, according to their respective responsibilities.

With reference to the management of relations and fulfillments towards public subjects, the control garrisons defined for the sensitive activity "Management of relations and fulfillments towards the Public Administration," to which reference is made (Section 5.1), must also be complied with insofar as applicable.

8.2. Management of employee and contractor expense reimbursements

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Review and approval of expense reports and related reimbursement • Verification of corporate credit card statements	• Head of Business Unit • Administration and Personnel • Project Manager • Order Manager • All employees and contractors who incur travel expenses	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration through the use of invoices or other documents for nonexistent transactions - Fraudulent declaration by other artifices • Offenses involving non-cash payment instruments (Article 25-octies.1) - Misuse and forgery of non-cash payment instruments

8.2.1. Specific principles of behavior

All employees and contractors must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Use the methods and means of payment (including corporate credit cards) allowed by internal practices;
- incur representation expenses exclusively for lawful purposes, in a transparent manner, in accordance with cost-effective and cost-containment criteria;
- request reimbursement only for expenses incurred in connection with work and which find adequate justification in relation to the type of assignment performed;
- To incur entertainment expenses proportionate to the company's goals and objectives;
- Immediately report any attempt to falsify and misuse non-cash payment instruments.

In addition, those who, by reason of their position or function, are involved in the verification and reimbursement of submitted expenses must:

- To manage the authorization and control of travel in a cost-effective and transparent manner, in compliance with internal regulations and current tax laws and regulations;
- Recognize reimbursement only for expenses incurred in connection with work and which find adequate justification in relation to the type of assignment performed;
- Ensure the disbursement of expense reimbursements only upon the applicant's submission of appropriate proof of expenditure.

It is also expressly forbidden:

- Pay or offer/promise payments or material benefits or gifts of money or other utility to public officials or public service officers or private counterparts or persons close to them to secure advantages of any kind to the Company;
- Follow up on undue requests for money or other benefits from any person. In such cases, the employee or collaborator must promptly inform his or her superior and suspend all business relations with the requester;
- incur and recognize entertainment expenses that may be interpreted as exceeding normal business practices or courtesy;
- Forging or altering non-cash payment instruments;
- Misuse (and/or encourage misuse by others who are not the holders) of credit or debit cards;
- Use/access computer equipment, devices or programs suitable for committing crimes involving non-cash payment instruments (e.g., acquiring the digital identity and payment data of third parties).

8.2.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the management of expense reimbursements.

In addition, as they are related to the sensitive activity in question, the following procedures/rules adopted by the Company are applied to supplement the reported control safeguards:

- Human capital management operations manual;
- PR04 "Project Management," with particular reference to the parts of the procedure concerning the management of mission expenses and other travel expenses incurred on projects by employees and contractors;
- PR07 "Timesheet/ CV Update/ Address Book," with particular reference to the part of the procedure concerning *timesheet* reporting on projects of travel expenses.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Verification and reimbursement of travel expenses are handled by Administration and Personnel.
- The allocation of corporate credit cards must be limited to cases of actual need and authorized in advance by the Administrative Body.
- The travel of employees and contractors must be authorized in advance by the Manager concerned, particularly, for job-related travel, by the Project Manager or Order Manager.
- The request for reimbursement must be made by the employee or collaborator through the use of the computer system in use (*timesheet* on the company dashboard), attaching to it the receipts for the expenses incurred.
- The employee's or contractor's supervisor, specifically, for job-related expenses, the project manager or order manager, verifies *timesheets* and approves travel expenses.
- Administration and Personnel verifies on a monthly basis, including on a random basis, the merit, appropriateness and presence of supporting evidence for the expenses submitted, processing the reimbursement request if successful.
- Administration and Personnel must verify the merit and appropriateness of expenses incurred via company credit card (through analysis of relevant card statements) on a monthly basis. Any anomalies should be verified with the person concerned, and any uncongruous amounts should be recharged.
- Expense reports of employees are reimbursed monthly through the relevant coupons, while those of freelancers are reimbursed with the payment of the relevant invoice. Reimbursement of expenses by cash, whatever the amount, is prohibited.
- The appropriate regulations governing, among others, travel and transfers must be attached to the contracts/letters of assignment concluded with the Company's employees.
- All relevant documentation under this sensitive activity is filed by Administration and Personnel.

9. P.S. E - LITIGATION MANAGEMENT

The sensitive activity that the Company considers relevant in litigation management is:

- Management of judicial and extrajudicial litigation (sec. 9.1).

9.1. Management of judicial and extrajudicial litigation

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Management of litigation and settlement agreements (including labor and tax litigation) • Management of relations with the Judicial Authority.	• Administrative Body • Compliance and Quality • Human Capital • Administration and Personnel • Head of Business Unit • Tender Office • All employees and contractors involved in any litigation or criminal proceedings	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases, including bribery in judicial acts - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Inducement not to make statements or to make false statements to judicial authorities (Art. 25-decies) • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent evasion of tax payment • Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy

9.1.1. Specific principles of behavior

All employees and contractors must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Promptly notify the Administrative Body of all acts, subpoenas and judicial proceedings (civil, criminal or administrative) involving them, in any respect, in connection with the work performed or related to it;
- Always make statements to the Judicial Authority that are true, complete, correct and representative of the facts;
- freely express their representations of the facts if investigated or charged in criminal proceedings;
- Promptly warn one's immediate supervisor of any threat, pressure, offer or promise of money or other benefit received for the purpose of altering statements to be made in criminal proceedings.

In addition, those who, by reason of their position or function, are involved in litigation management must:

- Comply with the power of attorney system in place;
- Ensure that the relations maintained with the Judicial Authority take place in absolute compliance with the laws and regulations in force as well as with the principles of loyalty, transparency and fairness;
- give full and immediate cooperation to the Judicial Authority, providing the requested documentation and information punctually and comprehensively;
- submit to individuals with appropriate powers, according to the current power of attorney system, the documentation in order to verify and approve it before submission to the Judicial Authority.

It is also expressly forbidden:

- Engage (directly or indirectly) in any activity that may favor or harm one of the parties to the litigation, in the course of civil, criminal or administrative proceedings;
- Exhibit false or altered documents;
- disclose in the documentation submitted for the purposes of the tax settlement procedure asset items in an amount lower than the actual amount or fictitious liability items;

- Simulately alienate or perform other fraudulent acts on the Company's assets suitable for rendering ineffective, in whole or in part, any compulsory collection procedure by the Tax Administration;
- Paying or offering, directly or indirectly, including in different forms of aid or contributions, payments or material benefits to officials of the Judicial Authority or persons close to them, in order to influence their behavior and ensure advantages of any kind to the Company.
- Conditioning or inducing, in any form or manner, the will of persons called to answer to the Judicial Authority in order not to make statements or make untrue statements;
- Promising or offering money, gifts or other benefits to persons involved in civil, criminal or administrative proceedings or persons close to them.

With reference to the management of relations and fulfillments towards the Judicial Authority, the principles of conduct defined for the sensitive activity "Management of relations and fulfillments towards the Public Administration," to which reference is made (Section 5.1), must also be complied with insofar as applicable.

9.1.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding any disputes.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Depending on the expertise, litigation should be handled, in each case with the support of external attorneys specializing in the subject matter and in coordination with Compliance and Quality:
  - by the Governing Body, with the support of the Heads of Business Units and, where applicable, the Tender Office, if they concern commercial aspects (with suppliers, customers, etc.) and/or contracting as well as any other civil, administrative or criminal matters other than those listed in the next point;
  - by Administration and Personnel, in coordination with the Administrative Body, if they concern tax issues;
  - by Human Capital, in coordination with the Administrative Body, if they concern labor law or occupational health and safety related issues.
- All Heads of Organizational Units involved must promptly notify the Administrative Body, Compliance and Quality, and the Head of the relevant Organizational Unit:
  - the certain or potential occurrence of passive litigation against the Company, providing the writs of summons received and all documentation necessary for the evaluation of the case;
  - the willingness to initiate active litigation, providing the reasons behind the request and all the necessary documentation for the evaluation of the case.
- The initiation of lawsuits, arbitrations, settlements or similar proceedings involving compensation or legal fees must be authorized by the Administrative Body, which also awards and revokes mandates to attorneys and technical consultants.
- As part of a court proceeding, the licensed attorney must issue a special power of attorney to an outside attorney specializing in the subject matter to grant special power of attorney to represent and settle.
- Exclusively appointed attorneys may interface with individuals involved in judicial proceedings or who are required to make statements before the Judicial Authority.
- The documentation to be submitted to the Judicial Authority (evidence, court documents, defense writs, etc.) is checked for correctness and accuracy by the Administrative Body or the Head of the relevant Organizational Unit, with the support of Compliance and Quality.
- Any settlement agreements must be authorized by the Administrative Body.

- The Administrative Body or the Head of the relevant Organizational Unit, at periodic budget closings, informs Finance and Budget of the status of outstanding litigation in order to be able to give due disclosure in the financial statements and calculate the allocation to the relevant provision for risks.
- All relevant documentation within the scope of this sensitive activity is filed by the Organizational Units from time to time competent according to the subject matter of the litigation.

10. P.S. F - MANAGEMENT OF GIFTS, DONATIONS AND SPONSORSHIPS

The sensitive activity that the Company considers relevant in the management of gifts, gratuities and sponsorships is:

- Management of gifts, donations and sponsorships (Sec. 10.1).

10.1. Management of gifts, donations and sponsorships

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Granting of gifts and gratuities • Management of sponsorships	• Administrative Body • Head of Business Unit • Office Coordinator	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, and self-money laundering (Article 25-octies) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration through the use of invoices or other documents for nonexistent transactions - Fraudulent declaration by other artifices - Fraudulent evasion of tax payment • Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater) and Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy - Associations for the purpose of terrorism, including international terrorism or subversion of democratic order

10.1.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Ensure that all gifts, donations and sponsorships are duly authorized in accordance with the proxy system in place and according to defined value thresholds, tracked and verifiable;
- Granting gifts and gratuities to third parties within the limits of commercial courtesy and modest value, as well as meeting criteria of reasonableness and expediency;
- ensure that the value, nature and purpose of gifts, donations and sponsorships are considered legal and ethically correct, such that they do not compromise the Company's image or are not interpreted as a means of obtaining favorable treatment for the Company;
- make disbursements in the form of donations or sponsorships solely to support initiatives worthy of protection and that do not conflict with the ethical principles of the Company.

It is also expressly forbidden:

- Making promises or undue gifts or other benefits to public officials or public service appointees or other third parties or persons close to them, for the purpose of promoting or favoring the interests of the Company or for the benefit of the Company;
- Giving gifts that could be interpreted as exceeding normal business practices or courtesy;
- Promising or making gifts for other than institutional purposes;

- disburse gifts, sponsorships or donations if there is a well-founded suspicion that this may expose the Company to the risk of committing one of the crimes governed by Legislative Decree 231/2001;
- Simulately alienate or perform other fraudulent acts on the Company's assets suitable for rendering ineffective, in whole or in part, any compulsory collection procedure by the Tax Administration.

With reference to the management of gift purchases, the principles of conduct defined for the sensitive activity "Procurement of goods and services, including professional appointments and consultancies," to which reference is made (para. 11.1), must also be complied with to the extent applicable.

10.1.2. Specific control measures

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding gifts, donations and sponsorships.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Gifts, donations and sponsorships must be approved in advance by the Administrative Body and may be proposed only by the Heads of Organizational Units (in addition to the Administrative Body) who must address requests to the Administrative Body itself in a formal manner, including by *e-mail.* Each request must state:
  - EXPECTED AMOUNT;
  - Name and role of the beneficiary;
  - motivation/purpose of the request.
- With particular reference to gifts, gifts of a total amount within the same calendar year in excess of 150 euros are not allowed towards the same recipient;
- With particular reference to donations and sponsorships, Office Coordinator performs checks, including reputational checks, on the counterparty and collects all necessary documentation to identify it (corporate data, financial statements, etc.). Donations may only be made to organizations and entities entitled to receive them under applicable laws and regulations. Donations should not be given to individuals, for-profit organizations, organizations other than charities or tax-preferred organizations.
- Only after formal approval by the Governing Body (including by *e-mail*), can the purchase of the gift, the contracting of the sponsorship, or the disbursement of the donation be made.
- A contract signed by a person with the necessary powers must be formalized against each sponsorship.
- The counterpart of liberal disbursements or sponsorships should be required to issue an appropriate receipt of payment.
- Office Coordinator, following a sponsorship, verifies the counterparty's actual fulfillment of the counterperformance.
- The list of gifts and donations given as well as sponsorships granted, with details of amount and beneficiary and any supporting documentation, must be filed by Office Coordinator.

With reference to the management of gift purchases, the control safeguards defined for the sensitive activity "Procurement of goods and services, including professional appointments and consulting services," to which reference is made (para. 11.1), must also be complied with to the extent applicable.

With reference to the management of payments of sponsorships and donations, the control safeguards defined for the sensitive activity "Management of financial and treasury operations and relations with financial institutions," to which reference is made (Section 7.2), must also be complied with to the extent applicable.

11. P.S. G - PURCHASING MANAGEMENT

The sensitive activity that the Company considers relevant in procurement management is:

- Procurement of goods and services, including professional and consulting appointments (Sec. 11.1).

11.1. Procurement of goods and services, including professional and consulting appointments

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Purchase of goods and services for job orders • Assignment of professional assignments within the scope of job orders • Procurement of headquarters goods and services, including consulting services	• Administrative Body • Head of Business Unit • Office Coordinator • Administration and Personnel • Project Manager • Order Manager	• Crimes against the Public Administration (Art. 25) - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, and self-money laundering (Article 25-octies) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Crimes against the individual (Art. 25-quinquies) - Illicit intermediation and labor exploitation • Crime of employment of third-country nationals whose stay is irregular (Art. 25-duodecies) • Crimes for the purpose of terrorism or subversion of democratic order (Art. 25-quater) and Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy - Associations for the purpose of terrorism, including international terrorism or subversion of democratic order • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration through the use of invoices or other documents for nonexistent transactions - Fraudulent declaration by other artifices

11.1.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Ensure that all purchases are duly authorized in accordance with the current power of attorney system;
- Ensure that the selection of suppliers, consultants and professionals is traceable, informed by criteria of objectivity and transparency, based on assessments of the quality and cost-effectiveness of the supply and professionalism of the counterparty;
- choose, whenever possible, from a shortlist of potential suppliers, consultants or professionals, the one that provides the best value for money;
- Carry out, where possible, specific checks in the presence of offers to supply goods at significantly below market prices, aimed at ascertaining the actual origin of the goods
- check in advance available information on suppliers, consultants and outside professionals in order to establish relationships only with parties who are financially sound, whose identity is certain, who enjoy

a good reputation, who are engaged only in lawful activities and whose corporate ethical culture is comparable to that of the Company;

- Always use the written form when awarding supplies, works, professional appointments and services;
- Ensure transparency of agreements and avoid entering into secret pacts or agreements contrary to the law;
- verify, prior to payment of the invoice, that the good or service was actually received in accordance with what was contractually agreed upon;
- Settle fees in a transparent manner that can always be documented and reconstructed *ex post*;
- Ensure the proper storage of all documentation produced and delivered in order to ensure traceability of the various stages of the process.

It is also expressly forbidden:

- Make purchases of goods, services, consultancy and professional services that are not reflected in a specific and justifiable need of the Company;
- Assigning supply assignments to persons or companies "close" or "liked" to public entities or any private counterparty with which the Company deals in the absence of the necessary requirements of quality and convenience of the transaction and professionalism;
- select professionals close to or suggested by public officials or any private third party, or pay them higher than due or market remuneration in order to secure advantages of any kind for the Company;
- establishing relationships or carrying out transactions with third parties if there is a well-founded suspicion that this may expose the Company to the risk of committing the crimes of criminal association, receiving, laundering or using money, goods or utilities of illegal origin, as well as self-money laundering;
- Paying, promising or offering, directly or indirectly, improper payments or other undue benefits to representatives of suppliers, potential suppliers, consultants and professionals, or persons close to them, for the purpose of promoting or favoring the Company's interests or for its benefit;
- Recognizing or promising money or other benefits to a third party (e.g., consultant, professional, etc.), or to a person traceable to the latter, in order to generate undue advantages in favor of the Company thanks to the intermediary work exercised by the latter towards a public official or person in charge of a public service by virtue of existing (because public and notorious) or boasted relationships;
- requesting or inducing representatives of counterparties involved in the process in question (e.g., suppliers and potential suppliers) to recognize or promise money or other benefits, for themselves, third parties or for the benefit of the Company, as the price of their illegal mediation with a public official or a person in charge of a public service or as remuneration in connection with the exercise of their functions or powers;
- in the purchase of contracted services, assign assignments to companies that do not show themselves to be in line with the principles of dignity, equality and welfare of each worker, and with respect to which there may be suspicion of direct or indirect recourse to non-regular, child or forced labor;
- employing, including through the contractor, workers or professionals, taking advantage of their state of need and subjecting them to exploitative conditions (e.g., through payment of wages in a manner manifestly different from the applicable collective bargaining agreements, repeated violation of regulations on working hours, rest periods, violation of safety and hygiene regulations in the workplace, subjecting them to degrading working conditions, surveillance methods or housing situations);
- Employ, including through the contractor, foreign workers or professionals whose stay in Italy is not legal;
- Approve invoices payable against non-existent services in whole or in part and/or unnecessary and/or at prices not in line with market prices;
- Make payments to suppliers, consultants or professionals without adequate justification;

- Recognize fees and expense reimbursements to suppliers, consultants or professionals that are not justified in relation to the type of task to be performed and market prices.

11.1.2. Specific control safeguards

The Company has adopted the following procedures for the management of procurement of goods and services as well as for the assignment of professional assignments to which all personnel who, by reason of their position or function, are involved in the sensitive activity must adhere:

- PR03 "Selection of Experts;
- PR04 "Project Management," with particular reference to the parts of the procedure dealing with the management of intercompany billing.
- PR05 "Procurement of miscellaneous goods and services."

The heads of the Organizational Units identified by corporate procedure PR14 "Information Flows and Attestations to the Supervisory Board" are also required to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the management of purchases.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

12. P.S. H - MANAGEMENT OF BUSINESS AND PROJECT ACTIVITIES

The sensitive activities that the Company considers relevant in the management of business and project activities are:

- Acquisition and management of orders (sec. 12.1);
- Management of external communication activities (sec. 12.2).

12.1. Acquisition and management of orders

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Participation in competitive bidding procedures or direct-tender requests for proposals issued by public entities • Acquisition of direct assignments with private clients • Operational management of job orders • Active reporting and billing	• Administrative Body • Head of Business Unit • Tender Office • Operational Control - Reporting • Tender Manager • Order Manager • Project Manager	• Crimes against the Public Administration (Art. 24 and 25) - Fraud against the State or other Public Entity - Computer fraud against the State or other Public Entity - Corruption against the Public Administration in its various cases - Undue inducement to give or promise benefits - Trafficking in unlawful influence - Fraud in public procurement • Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals • Crimes against industry and trade (Art. 25-bis.1) - Disturbed freedom of industry or commerce - Fraud in the exercise of trade - Unlawful competition by threat or violence • Receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, and self-money laundering (Article 25-octies) - Receiving - Recycling - Use of money, goods or utilities of illicit origin - Self-money laundering • Organized crime offenses (Art. 24-ter) - Conspiracy, including transnational conspiracy • Tax crimes (Art. 25-quinquiesdecies) - Fraudulent declaration by other artifices - Issuance of invoices or other documents for non-existent transactions

12.1.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Operate in compliance with applicable national and international laws, regulations and rules on public bidding;
- Operate in compliance with national and international *antitrust* and competition protection laws;
- Comply with the power of attorney system in place;
- Ensure that the selection and management of customers and any business *partners is carried out by* the relevant Organizational Units, so that transactions are carried out with contractual counterparties who can guarantee integrity, honesty and reliability in the management of business relations, as well as financial and asset soundness;
- Maintain fair, transparent, impartial and cooperative relations with representatives of public or private entities when participating in tenders or requests for bids and following awarding of contracts;

- Use, in formal and informal contacts with business counterparts, diligent and professional conduct so as to provide clear, accurate and truthful information;
- To base its behavior on criteria of honesty, courtesy, transparency and cooperation, providing adequate and complete information about its business offerings, avoiding elusive or corruptive practices or threats and violence aimed at influencing customer behavior.
- Ensure that the documentation sent or shared with clients is always complete, truthful and correct;
- report without delay to its hierarchical manager any conduct engaged in by persons operating within the counterparty, aimed, for example, at obtaining favors, illicit handouts of money or other benefits, as well as any critical issue or conflict of interest that arises within the relationship with the customer or potential customer, at the same time suspending all business relations with the same;
- provide its employees and collaborators with adequate directives on how to conduct themselves in formal and informal contacts with Public Administration officials and representatives of private clients when participating in tenders or requests for tenders and following awarding of contracts;
- Ensure that the establishment and application of costs and tariffs to customers are carried out in accordance with principles of fairness, transparency and impartiality;
- ensure that the bid corresponds to services that can actually be procured and that the Company is capable of performing;
- Ensure that, if awarded the tender/bid, the services rendered meet all the characteristics declared in the tender/bidding process;
- To refrain from improperly influencing the decisions of the other party especially with regard to the exercise of evaluative activities in the context of awarding a tender or request for proposal;
- Report and prevent any conflicts of interest with current or potential clients.

It is also expressly forbidden:

- Sign tender/tender acts or documents in the absence of formally assigned powers;
- Putting in place transactions that are suspicious in terms of fairness and transparency;
- Issue invoices receivable for services that are wholly or partially nonexistent or for amounts different from what is contractually stipulated;
- Giving or receiving undue or unjustified payments (in whole or in part) and the like aimed at creating slush funds or extra-accounting availability;
- Define relationships with individuals or legal entities that intentionally do not adhere to the ethical principles of the Company;
- Corresponding or offering, directly or indirectly, including under different forms of aid or contributions, payments or material benefits to exponents of the counterparty or persons close to them, in order to influence their conduct and ensure advantages of any kind to the Company when participating in tenders or requests for tenders and following awarding of contracts;
- Yielding to recommendations or pressure from counterparty representatives when bidding or requesting bids and following an award;
- Engaging in misleading conduct toward the counterparty such as to mislead the counterparty;
- Omit due information or submit untrue documents and statements in order to steer the other party's decisions in their favor;
- Accepting money, gifts or offers of other benefits or advantages of any kind, from anyone, that are connected with or related to the performance of one's duties;
- where tender fulfillments are carried out using the Public Administration's computer/telematic system, alter the same and the data entered, or improperly or illegally use the data processed, causing damage to the Public Administration itself;

- Directing bidding/tender procedures for the procurement of supplies in order to make a specific party the successful bidder, including artificially excluding other participating parties;
- Gain an unfair advantage over anyone through illegal business practices;
- Engaging in conduct, either directly or through an intermediary, aimed at influencing the price of products, discouraging the participation of other bidders in tenders/requests for bids, or obtaining any information useful for procuring an unfair advantage to the detriment of other parties involved.
- Engaging in conduct that, by means of violence or threats, or by gifts, promises, collusion or other fraudulent means, is intended to prevent or disrupt public tenders or private bids on behalf of public administrations, or to remove bidders from them;
- Engaging in conduct that, through violence or threats, or by means of gifts, promises, collusion or other fraudulent means, is aimed at disrupting the administrative procedure aimed at establishing the content of the call for tenders or other equivalent act in order to condition the manner in which the Public Administration chooses a contractor.

With reference to contract purchases (professional services, etc.), the principles of conduct defined for the sensitive activity "Procurement of goods and services, including professional appointments and consultancies," to which reference is made (para. 11.1), must also be complied with insofar as applicable.

12.1.2. Specific control safeguards

The Company has adopted the following procedures in the area of contract acquisition and management to which all personnel who, by reason of their position or function, are involved in the sensitive activity must adhere:

- PR02 "Tendering;
- PR04 "Project Management;
- PR06 "Business Interaction;
- PR07 "Timesheet/ CV/ Address Book Update," with particular reference to the time and expense accounting of employees and contractors on job orders;
- PR13 "Customer Satisfaction.

The heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" are also obliged to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the acquisition and management of orders.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

With reference to contract purchases (professional services, etc.), the control principals defined for the sensitive activity "Procurement of goods and services, including professional appointments and consultancies," to which reference should be made (para. 11.1), must also be complied with insofar as applicable.

12.2. Management of external communication activities

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Management of the institutional website and other promotional and outreach tools (including *social* channels) • Preparation and dissemination of promotional materials and news related to the Company (releases, *newsletters,* etc.)	• Administrative Body • Communication	• Copyright infringement crimes (Art. 25-novies)

12.2.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Operate in compliance with current copyright protection regulations;
- Comply with the current proxy system;
- Ensure the constant monitoring of and compliance with national and international regulations placed on the protection of copyright and the rights associated with the reproduction and public performance of copyrighted works, and promote the proper use of all intellectual works of a creative nature;
- Ensure that for all content on the network by third parties or purchased by the Company and placed on the network, there is an express assumption of responsibility by such third parties regarding compliance with copyright and other rights related to the use of intellectual works.

It is also expressly forbidden:

- Misuse copyrighted material where you do not hold exclusive ownership and/or legitimate title to the use.

With reference to purchases of promotional materials, the principles of conduct defined for the sensitive activity "Procurement of goods and services, including professional appointments and consultancies," to which reference is made (para. 11.1), must also be complied with insofar as applicable.

12.2.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding external communication.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- External communication activities are handled exclusively by Communication under the coordination of the Administrative Body.
- All communication material must be verified by Communication (in terms of the accuracy of the information included and, where applicable, possession of the relevant right of use) and approved by the Governing Body prior to its disclosure or publication.
- Communication, in the possible acquisition of editorial, photographic, audiovisual, etc. content from third parties, must obtain, where applicable, authorizations for use (copyright assignment contract from the author; signing of releases from the filmed subjects or holders of reproduction rights to the filmed locations).
- Contracts/letters of assignment entered into with outside consultants, companies or agencies that may support LKIBS in the production and dissemination of editorial, photographic, audiovisual, etc. content must include, among others, a hold harmless clause in favor of LKIBS to hold it harmless from any copyright claims;
- All relevant documentation within the scope of this sensitive activity is archived by Communication.

With reference to the purchase of promotional materials, the control principals defined for the sensitive activity "Procurement of goods and services, including professional appointments and consulting services," to which reference is made (para. 11.1), must also be complied with insofar as applicable.

13. P.S. I - INFORMATION SYSTEMS MANAGEMENT

The sensitive activity that the Company considers relevant in the management of information systems is:

- Management and use of company and third-party information systems (sec. 13.1);

13.1. Management and use of company and third-party information systems

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Managing access to data and systems • *Backup* management • Enterprise *software* management • Security management (network and physical)	• Administrative Body • IT manager of reference for: - ICT infrastructure management (external contact person) - management of the Corporate Dashboard • All employees and contractors using Company computer systems or accessing third-party computer systems	• Crimes against the PA (Art. 24) - Computer fraud • Computer crimes and unlawful data processing (Art. 24-bis) - Unauthorized access to a computer or telecommunications system - Unlawful interception, obstruction or interruption of computer or telematic communications - Unauthorized possession, dissemination and installation of equipment and other means of intercepting, preventing or interrupting computer or telematic communications - Damage to information, data and computer programs - Damage to information, data and computer programs used by the State or other public agency or otherwise of public utility - Damage to computer or telematic systems - Damage to computer or telematic systems of public utility - Unauthorized possession, dissemination and installation of equipment, codes and other means of access to computer or telematic systems - Unauthorized possession, dissemination and installation of computer equipment, devices or programs intended to damage or disrupt a computer or telecommunications system - Forgery of computer documents • Crimes involving non-cash payment instruments (Art. 25-octies.1) - Computer fraud that produces transfer of money, monetary value or virtual currency (Art. 640-ter para. 2, Criminal Code) • Copyright infringement crimes (Art. 25-novies) • Tax crimes (Art. 25-quinquiesdecies) - Concealment or destruction of accounting documents

13.1.1. Specific principles of behavior

All employees and contractors, in using company or third-party computer systems must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the system of e proxies in place;
- comply with the rules and principles referred to in the document "Vademecum for the Use of Information Systems and Data Protection," which defines the purposes and methods of use of the information systems made available by the Company

It is also expressly forbidden:

- Engaging in conduct, including with the help of third parties, aimed at accessing others' computer systems with the goal of:
  - Abusively acquiring information;
  - Damage destroy data;
- Abusively use access codes to computer and telecommunications systems as well as proceed to disseminate the same;
- engage in conduct aimed at destroying or altering computer documents having evidentiary purposes (e.g., financial statements, attestations or self-certifications directed to public bodies, documents created

with the aid of digital signature tools, etc.) in the absence, where permitted by law, of specific authorization;

- Use or install programs other than those authorized by the IT Manager and unlicensed;
- Installing, duplicating, or disseminating to third parties programs (*software*) without having the appropriate license or exceeding the rights allowed by the purchased license (e.g., maximum number of installations or users);
- Make illegal *downloads* or transmit copyrighted content to third parties;
- Saving unauthorized or copyright-infringing content or *files* on company memory drives;
- circumvent or attempt to circumvent the Company's or third parties' security systems (e.g., *Antivirus*, *Firewall*, *Proxy server,* etc.);
- Engaging in conduct aimed at destroying or altering company or third-party computer systems;
- Enter the corporate network and programs with a different user identification code than the one assigned;
- Abusively hold or disseminate access codes to computer or telecommunications systems of third parties or public agencies;
- Disclose to others (except as formally delegated) or misuse assigned digital signature tools;
- Illegally intercept, prevent or interrupt computer or telematic communications;
- Alter in any way the operation of a computer or telematic system of the Public Administration or private third parties, or intervene without right in any manner on data, information or programs contained in a computer or telematic system of the Public Administration or private third parties, in order to procure an advantage for the Company.

The IT Manager puts in place the necessary actions to:

- Check the security of the company's network and computer systems and protect data security;
- Identify potential vulnerabilities in the system of IT controls;
- Evaluate the proper technical implementation of the corporate power system at the level of information systems and user enablement traceable to proper segregation of duties;
- monitor organizational or technical changes that could result in exposure of the information system to new threats, making the access control system inadequate;
- Monitor and carry out necessary access management activities to corporate and third-party information systems;
- Ensure that only original, duly authorized or licensed *software is* installed for all users;
- Ensure that the logical and physical security of the Company's information systems is managed in accordance with internal rules and by constantly maintaining and updating the infrastructure components (*hardware* and *software*) that guarantee their effectiveness;
- Define and enforce rules for all users to ensure that *passwords* on different business applications are updated according to defined business rules and in line with regulatory requirements;
- monitor the proper application of all measures deemed necessary in order to deal specifically with computer crimes and unlawful data processing;
- Prevent access to restricted areas (e.g., *server* rooms, technical rooms, etc.) by unauthorized persons;
- Ensure that the activities carried out by third-party vendors regarding:
    - *networking* (e.g., management of dedicated CED infrastructure services, network components, security, *backup*);
    - connectivity;

  comply with corporate principles and rules in order to protect data security and proper subject access to application and infrastructure systems.

13.1.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding the management and use of IT tools.

In addition, as they are related to the sensitive activity in question, the following rules adopted by the Company are applied to supplement the reported control safeguards:

- ICT Handbook;
- Vademecum for the use of Information Systems and data protection.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

General principals

- The company's IT systems and the rules for access and use thereof (as well as the IT systems of third parties) by employees and contractors are managed, under the coordination of the Administrative Body, by the relevant IT Manager.
- All relevant documentation within the scope of this sensitive activity is archived by the relevant IT Manager who provides copies (if necessary, also upon request) to the Administrative Body.

Managing access to data and systems

- The relevant IT Manager shall ensure a structured and formalized process for the creation, modification and deletion of users in the event of commencement, change or termination of employment or duties, as well as a system of access profiling according to the role assigned and position held. Access to information residing on company and third-party *servers* and databases must be restricted by appropriate authentication tools including, but not limited to:
  - Use of *accounts* and *passwords*;
  - Profiled access to network folders.
- The creation or modification of a new user account can only be carried out by the relevant IT Manager, subject to the formal authorization (including by *e-mail*) of the Manager of the employee or collaborator concerned, who must ensure that the profiling is consistent with the role performed and the position held.
- In the event of termination of employment, the Manager of the affected employee or collaborator, or Human Capital, shall notify the relevant IT Manager who shall promptly proceed to deactivate the user.
- Annually, the relevant IT Manager must perform, with the support of the relevant Organizational Units, a review of users and profile changes.
- The Line Manager of the concerned employee or collaborator must ensure the proper assignment/enabling of access to third-party (public or private entities) sites or programs that require access credentials (*user-id*, *password* and/or *Smart Card*).
- The characteristics and methods of updating individual user *passwords* on the various business applications must be ensured by the application of specific rules defined by the relevant IT Manager (in any case, the *password* must meet specific security and complexity requirements and must be changed periodically).
- Access to systems as a "system administrator" should be limited to only authorized personnel identified by the Administrative Body.
- Each employee or collaborator is provided with a named e-mail address for work use only.
- Connections to the system remotely can be made only through secure communication channels (*VPN*).

- For mobile *device management*, a *Mobile Device Management tool* must be used.
- Only authorized business figures should be allowed to use digital signatures.

Backup management

- All *files*, programs and operating systems must undergo a regular *backup* procedure managed by the relevant IT Manager.
- *Backup* media are stored in a different location than where the *servers are* installed.
- The relevant IT Manager must perform periodic verification activity on both the integrity of the *backup* media and the correct outcome of the *backup* media.

Enterprise software management

- Users cannot be administrators of the *personal computers* in use.
- The activity of installing *software* on employees' workstations is permitted only to the IT Manager for ICT infrastructure and after verification of possession of the necessary licenses.
- The IT Manager for ICT Infrastructure must periodically verify that all programs installed on company and third-party workstations are validly licensed.

Security management (network and physical)

- The internal network must be protected by appropriate access restriction tools (*firewalls*) managed by the IT Manager for ICT infrastructure.
- Enterprise computers must be encrypted by the IT Manager for ICT infrastructure before delivery to relevant users.
- *Servers* and *clients* must be protected against potential external attacks through the use of specific *antivirus software* that performs incoming checks and updates automatically. The IT manager for ICT infrastructure must ensure that they are always up-to-date and ensure monitoring activity on network equipment.
- The e-mail *server* should be equipped with *spamming*, *anti-phishing* and *anti-virus* filters.
- *Internet* access should be filtered through an automatic *web content filtering* system.
- The IT Manager for ICT Infrastructure periodically conducts vulnerability *assessment* and *penetration testing* activities aimed at identifying potential vulnerabilities in systems and applications.
- Wi-Fi networks are protected and accessible: (i) to corporate devices, subject to authorization by the IT Manager for ICT Infrastructure, with user authentication; (ii) to devices used by authorized visitors (suppliers, consultants, employees, etc.) by the IT Manager for ICT Infrastructure and only for the duration of their stay in the company, through a special registration procedure (*guest* network).
- The Administering Body must implement appropriate security measures to prevent unauthorized access to the CED room (use of key or *badge*, etc.) as well as damage (fire protection system, etc.).

14. P.S. M - QUALITY, OCCUPATIONAL HEALTH AND SAFETY AND ENVIRONMENTAL COMPLIANCE MANAGEMENT

The sensitive activities that the Company considers relevant in the management of occupational and environmental health and safety compliance are:

- Management of occupational health and safety compliance (sec. 14.1);
- Management of environmental compliance (sec. 14.2);
- Management of relations with private certifying bodies (sec. 14.3).

14.1. Management of occupational health and safety compliance.

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Verification of compliance with legal technical and structural standards relating to equipment, facilities, workplaces as well as chemical, physical and biological agents • Risk assessment and preparation of relevant prevention and protection measures • Activities of an organizational nature, including emergencies, first aid, contract management, periodic safety meetings, consultation with workers' safety representatives • Procurement and supply management • Health surveillance activities • Information and training of employees and contractors • Supervisory activities and reference to workers' compliance with safe work procedures and instructions and verification of their implementation • Implementation of registration systems and acquisition of legally required documentation and certifications • Surveillance and disciplinary system	• Administrative Body (Employer) • External Prevention and Protection Service Manager (RSPP) • Physician-in-Charge (MC) • Occupational health and safety officers (proxies) • Emergency management team (firefighters" and "first aid officers) • Workers' Safety Representative (RLS) • All workers (employees and contractors)	• Occupational health and safety offenses (Art. 25-septies) - Manslaughter - Negligent personal injury

14.1.1. Specific principles of behavior

All employees and contractors of the Company must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- comply with the obligations set forth in Legislative Decree 81/2008, as amended, regarding health and safety at work as well as scrupulously observe the provisions and instructions given by the persons in charge in order to preserve their own and all workers' health and safety;
- Comply with the power of attorney system in place;
- Cooperate, including through their representatives, in the assessment of occupational safety and health risks, including interference risks, with respect to standard tasks and workplaces presse the LKIBS premises and offices;
- Promptly report to the identified structures and in the manner defined by them, any situations of danger and risk, accidents, occupational diseases, near *misses* (or near *misses*), incidents that have occurred (regardless of their severity), and violations of rules of conduct and company procedures and practices;
- Use, according to instructions, equipment in the workplace, as well as means of transport and safety and protective equipment, where provided;

- Do not remove or modify machine and equipment safety devices or other signaling or control devices in any way;
- not to carry out on their own initiative operations or maneuvers that may compromise their own or other workers' safety or that may expose themselves, their colleagues or third parties to dangerous situations;
- Report any anomalies, situations, or safety and health hazards that are different from those known or particularly significant;
- Comply with behavioral practices and guidelines for managing occupational safety and health in all company activities;
- Effectively participate in educational and training sessions organized by the Company on occupational health and safety risks;
- Review the occupational health and safety information delivered by the Company prior to the start of each business activity and adhere to the principles of behavior required by LKIBS.

Those who are specifically responsible, at the Company's locations and offices located throughout the country, for occupational health and safety compliance must also:

- Maintain up-to-date and continually comply with the regulatory body and the system of proxies and powers of attorney in the areas of safety, accident prevention and hygiene;
- Pursue the goal of "no harm to people."
- Promote a culture in which all employees and contractors participate in this commitment;
- ensure the suitability of human resources-in terms of number, professional qualifications and training- and materials, necessary to achieve the objectives set by the Company for maintaining and/or improving the levels of worker safety and health;
- Ensure the acquisition and management of the company's means, equipment, facilities and, in general, facilities in compliance with the technical and structural standards of the law, including through a continuous process of maintenance (ordinary and extraordinary) of the same;
- Define goals for worker safety and health and identify risks;
- Ensure an adequate level of training and information to employees and collaborators on the safety management system defined by the Company and the consequences of non-compliance with the legal regulations and the rules of behavior and control defined by the Company;
- require that an adequate level of education, training and information be provided by the Employer-Contractor to the workers of the third-party contracting/subcontracting firms to the extent of their competence and with regard to interference risks, on the safety management system defined by the Company and on the consequences of non-compliance with the legal regulations and the rules of behavior and control defined by the Company itself;
- Promptly report to the structures identified in accordance with the law and/or internally any signs / events of risk / danger regardless of their severity.

14.1.2. Specific control safeguards

The Company has adopted the following procedures for managing occupational health and safety compliance:

- PR08 "Security Locations;
- PR10 "Internal Audits.

The above procedures are intended to regulate aspects relevant to occupational health and safety management so that at LKIBS:

- specific objectives are planned for the pursuit of the health and safety policy with an indication of the resources dedicated to them;
- a risk identification and assessment activity with the definition of control actions and areas for improvement is prepared and implemented;

- are defined and communicated in the company the names and responsibilities of those responsible for worker health and safety compliance;
- information, education and training actions are implemented;
- procedures are implemented for communication within the organization and for worker participation and consultation in relation to occupational safety and hygiene obligations;
- improvement and corrective actions are taken to ensure ongoing compliance of the adopted management system on worker health and safety, following appropriate monitoring activities.

In addition, the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" are also required to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding aspects related to occupational health and safety.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

In light of this premise, compliance with all required and applicable occupational health and safety obligations must be ensured, including, with reference to Article 30 of Legislative Decree 81/2008, the specific control garrisons below.

Verification of compliance with legal technical and structural standards relating to equipment, facilities, workplaces as well as chemical, physical and biological agents[1]

The Employer, in cooperation with the RSPP, shall ensure:

- Identify, also following the drafting of the Risk Assessment Document (DVR) and subsequent updates, any improvement actions related to the compliance, with respect to the technical-structural standards of the law, of equipment (by way of example only, lifting equipment both its own and that of third parties), facilities (by way of example only, thermal and electrical systems, earthing, fire prevention both its own and that of third parties), workplaces, chemical, physical and biological agents, and related implementation responsibilities, with reference to both the Company's headquarters and executive and administrative offices;
- Carry out periodic inspections of workplaces where activities are carried out, aimed at ensuring that legal standards are maintained over time;
- Define the safety requirements to be checked by the relevant Organizational Units prior to the procurement of equipment, facilities, chemical, physical and biological agents;
- Ensure continuous monitoring of the development of structural-technical standards and regulations.

Risk assessment and preparation of relevant prevention and protection measures

The Employer, in coordination with the RSPP and with the support of the appointed health and safety officers (*primarily* the MC and the RLS), the various relevant company managers and the heads of the relevant offices, must carry out an assessment of the health and safety risks to the organization in order to identify and implement preventive and worker protection measures, reducing the hazards and related risks to acceptable measures, in relation to the knowledge acquired and the priority defined.

This analysis is formalized in a special document (DVR), as required by Legislative Decree 81/2008, as amended (Testo Unico sulla Sicurezza - TUS), and further current legislation on occupational health and safety, containing, among other things, the identification and assessment of risks for each company task, prevention and protection measures and individual protection devices assigned to each employee as well as the provisions of Article 28 paragraph 2 letters a) to f) of Legislative Decree 81/2008, signed by the Employer.

Therefore, the Employer shall, in cooperation with the aforementioned company contact persons and subject to any delegation, where permitted by law, to:

[1] This requirement also applies to machines and equipment that are possibly used at production sites (even if such equipment is hired out).

- Evaluate all risks associated with the activity, including interference risks, risks related to work-related *stress*, and those concerning pregnant workers, and prepare and formalize the risk assessment document;
- update the DVR as a result of organizational and procedural changes, technical changes, changes necessitated by regulatory developments, as well as following significant accidents, incidents and near misses and/or health findings that highlight the need, within a short period of time and in any case no later than one month after the change is made;
- Formalize a specific risk assessment for each task and/or activity carried out in the offices, with identification and assessment of each specific hazard, associated risk and measures for its mitigation and reduction;
- Guarantee:
  - The right of access and use, without cost, for each worker to appropriate personal protective equipment (PPE) appropriate to the task performed;
  - The continuous updating of a personal logbook/fiche summarizing the safety equipment assigned to workers;
  - The methodologies for incident analysis and classification;
  - The definition of responsibilities for implementing measures to mitigate consequences as a result of accidents or nonconformities, as well as for initiating and completing corrective measures.

With reference to the management of activities and services provided by third parties at the Company's headquarters and at workplaces outside the offices (whether or not they are under the direct control of the LKIBS organization) before starting the work, the elaboration, (in coordination with the Employer(s) of the third party company(ies) and/or the subcontracting/subcontracting companies) of a document must also be carried out, to be annexed to the contract, indicating the measures taken to eliminate or, where this is not possible, minimize risks from interference, in order to promote cooperation and coordination among employers, also providing for the estimation of the related charges of preventive and protective measures aimed at the safety and health of workers.

This document, depending on regulatory requirements, may take the form of:

- Safety and Coordination Plan (PSC), in the case of contracts that fall under the scope of Title IV of Legislative Decree 81/2008. It is prepared by the Design Phase Safety Coordinator (CSP), appointed by the client entity;
- SOP (Operational Safety Plan), provided by third parties under contract that may fall under the scope of Title IV of Legislative Decree 81/2008. It is signed by the Employer of the contractor company and delivered to the Principal of LKIBS for the appropriate legal requirements;
- DUVRI, for the remaining types of contracts. It is drafted, where required by Art. 26 of the TUS, by the commissioning Employer, in collaboration with the relevant parties. The DUVRI is also prepared and shared with contractors for the management of contract risks (e.g., maintenance) present at the company's offices.

Activities of an organizational nature, including emergencies, first aid, contract management, periodic safety meetings, consultation with workers' safety representatives

The organization has a system of appointments that defines responsibilities, duties and powers regarding safety, accident prevention and occupational hygiene. The Employer must provide for the appointment of the RSPP and MC and must designate in advance the workers in charge of the implementation of fire prevention measures, evacuation of workplaces in case of serious and immediate danger, rescue, first aid and, in any case, emergency management (First Aid Officers and Fire Emergency Officers, etc.). To support emergency management, a specific Emergency Plan is drawn up for each office and periodic emergency drills are also carried out while, at workplaces outside the offices, information on the emergency plans and procedures of the companies responsible for the aforementioned sites are acquired and shared.

Should the Employer decide to make use of one or more Delegated Employers or Safety Managers, he/she shall appoint them specifically through specific delegation and with his/her own autonomy of expenditure.

In addition:

- all persons in charge of occupational safety identified above must exercise, for the area of their responsibility, all powers granted and fulfill all obligations under Legislative Decree 81/2008, as amended, and all other applicable safety, accident prevention and environmental hygiene laws and regulations;
- the Employer must adopt specific procedures for defining, documenting, and communicating the roles, responsibilities, and faculties of those who manage, perform, and verify activities that affect health and safety risks (by way of example: appointment of supervisors, appointment of the RSPP, communication regarding the election of the RLS by workers, appointment of the MC and its communication, appointment of first aid officers and fire emergency officers and their communication);
- in case of the absence of the personnel in charge, with reference to the management of emergencies and the provision of first aid, the RSPP and the relevant Organizational Units shall define the communication methods so as to promptly inform the Prevention and Protection Service.

In particular, the Employer shall, with the support of the RSPP and other competent contacts (including the MC), subject to any delegations where permitted by law, define, issue and disseminate to all workers, at least with respect to the risks defined in the DVR, service orders, instructions and/or operating procedures aimed at:

- Ensure health and safety in the workplace, with reference to both offices and administrative offices whether or not they are under the direct control of LKIBS;
- Manage contracting and subcontracting activities and related interference risks;
- Regulating information flows;
- Give delegated persons in safety and health management the spending autonomy necessary to carry out the delegated functions and the necessary powers of organization, management and control;
- Ensure the performance of operational activities and define instructions to properly and safely carry out activities related to each professional figure in the Entity;
- Ensure proper management of emergency situations and provide for periodic emergency testing;
- To define the operating procedures to be followed in contracting out work to third parties in order to ensure adequate prevention and protection conditions in accordance with current regulations.

The Employer, with the support of the RSPP, the appointed health and safety individuals, the various company managers of competence and, if necessary, professionals specialized in the field, must ensure all the requirements of Legislative Decree 81/2008, as amended, and in particular:

- convene, as required by Article 35 of Legislative Decree 81/2008, at least once a year a meeting attended by the Employer, RSPP, MC and RLS;
- Ensure the recording of the performance of the above activities, as well as the archiving of related documentation.

At the meeting, the Employer shall submit at least the following topics for consideration by the participants:

- The risk assessment document and the resulting prevention measures;
- trends in occupational accidents and diseases and health surveillance;
- The selection criteria, technical characteristics and effectiveness of personal protective equipment;
- programs to inform and train employees for the purpose of safety and protection of their health;
- audit activities.

Procurement and supply management

The qualification process of suppliers carried out by the organization requires the request and verification (in any case at the first qualification stage, with defined periodicity in case of continuous and/or repeated supplies over time), also with the support of the RSPP, of the possession of the requirements of technical and professional suitability of the contractor or self-employed workers to carry out the activity as well as the acquisition of specific documentation such as registration with the Chamber of Commerce, the declaration of

the absence of disqualification measures according to Art. 14 of Legislative Decree 81/2008, indication of the name(s) of the person(s) in charge of carrying out the tasks referred to in Art. 26 of Legislative Decree 81/2008, as amended (indicating the specific duties, DURC or INAIL position, DVR, duties, work experience and INAIL position), the appointments of the Prevention and Protection Service Manager and the Competent Doctor.

The Employer, with the cooperation of the RSPP and safety officers, will ensure during the execution of the work:

- Cooperation between employers in the implementation of measures for prevention and protection from occupational hazards of accidents on the work activity covered by the contract;
- Coordination of protective and preventive measures against the risks to which workers are exposed (employers should also inform each other in order to reduce risks due to interference - should they arise - between the work of different companies involved in the execution of the overall work);
- That LKIBS personnel not involved with the contract be trained/informed not to interfere with the work of outside personnel engaged in the work, not to lend support and not to use the work equipment of the contracting companies in any way.

These obligations also apply with specific reference to activities and workers working at external workplaces for consulting activities.

In particular, in the case of contracts falling under Title IV of Legislative Decree 81/2008, the Client will carry out all the tasks required by the regulations including appointing the Safety Coordinator during execution (CSE), who will verify compliance with the requirements contained in the Safety and Coordination Plan (PSC) during the period of site activity.

Health surveillance activities

It is the responsibility of the Employer to ensure that the MC has the necessary conditions for conducting health surveillance of workers employed by the organization, providing it with the appropriate space for performing the activity under its responsibility and for recording the fulfillment of the legal obligations set out below as well as for storing the relevant documentation.

The Employer shall, with the support of the RSPP and MC:

- To update the injury statistics;
- To the definition of responsibilities inherent in the investigation following accidents and/or injuries.

It is the MC's responsibility, provided it is not at the expense of the mandatory assessments required by law, to assess the adequacy and, if necessary, update the surveillance program according to any changing needs.

In particular, the MC must, as stipulated in Article 25 of Legislative Decree 81/2008, among other things:

- Cooperate with the Employer in risk assessment;
- plan and carry out:
  - (i) preventive examinations designed to ascertain the absence of contraindications to the work for which workers are intended, for the purpose of assessing their suitability for the specific task,
  - (ii) periodic examinations, aimed at checking the health status of workers and expressing the judgment of suitability for the specific task;
- Establish, update and maintain the health and hazard records of each worker;
- visit the workplaces once or twice a year according to legislative dictates and produce relevant minutes of the inspections carried out;
- formalizing and communicating to the worker the outcome of the tests conducted, containing judgments of suitability or unfitness, issuing two copies (one to the worker and one to the Employer also for relative archiving);
- Participate in the periodic safety meeting under Art. 35 of Legislative Decree 81/2008, reporting on the visits made, trends in occupational injuries and diseases etc.

Health surveillance obligations refer to the organization's employees, given that collaborators and other third-party personnel involved are required to implement related obligations on their own initiative.

To facilitate this compliance, the organization promotes awareness and training to third-party collaborators, etc.

Information and training of employees and contractors

The Employer shall, with the support of the RSPP and the relevant Organizational Units to:

- Prepare the Annual Training and Education Plan with identification of training needs to staff;
- Organize and deliver education/training programs to newly hired workers/subject to job change;
- Organize and deliver specific and periodic training programs divided by areas of membership (medical, administrative, etc.) and for particular groups (e.g., firefighting and first aid);
- record training activities on appropriate media and keep summary tables of the training carried out during the year with related documentation (participant attendance sheets, any learning and appreciation verification sheets, training materials distributed);
- Conduct periodic audits to ascertain the level of learning and awareness in the area of worker safety, formalizing and archiving the results, after sharing with the RLS;
- Organize emergency simulation tests (e.g., evacuation tests) at least annually at the offices;
- provide suppliers and contractors with detailed information on the specific risks existing in the Company's premises/offices as well as the behavioral and control rules adopted by the Company, defined in this document and in the Company's procedures;
- Ensure the recording of the performance of the above activities, as well as the storage of related documentation and the evaluation of its effectiveness;
- Provide the necessary education, information and training for workers following regulatory updates and following organizational, technical or procedural changes with an impact on work activity for safety purposes.

These activities also apply with reference to the tasks performed by workers not employed by the organization (e.g., contractors) at workplaces where company activities are carried out; in such cases, specific information must be distributed to all (employees and non-employees alike) that states the possible occupational health and safety risks and the rules and behaviors that everyone must compulsorily follow.

Supervisory activities and reference to workers' compliance with safe work procedures and instructions and verification of their implementation

The Employer supervises the proper performance of the delegated activities and, through the cooperation of the Managers and Supervisors, each within the scope of their responsibilities, the compliance by workers with their legal obligations and the company's occupational health and safety regulations. Supervision is also carried out through the inspections carried out within the scope of their duties, at offices and premises, by the RSPP and the MC.

In addition, the Employer periodically assesses the need to plan and implement, also using third-party expertise and consultants, the necessary internal audit activities to verify compliance with the requirements defined in the procedures, guidelines and other documentation of the Health and Safety Management System. Any anomalies or nonconformities found during the audits are managed and resolved with a formalized corrective and preventive action plan indicating when, how and who is responsible.

For audit interventions, the Employer shall ensure that:

- on the basis of an "audit plan" prepared by the RSPP, carries out periodic audit activities on the safety management system, with the possible support of formally appointed external professionals in compliance with the behavioral and control rules defined in this Model.
- Approves the annual audit plan, which must include actions aimed at verifying compliance with the standards by all components of the organization;
- examines and carries out checks on the minutes of the periodic audits related to the verification interventions and, in particular, on the findings that have emerged (nonconformities and/or observations) and the related action plan (defined by the area/department being audited with the support of the person

who carried out the audits), in which the actions necessary to remove the nonconformities found, the person responsible for their implementation and the timeframe are indicated;

- Approves the action plan;
- the RSPP checks the progress of the action plan by promptly notifying the Employer of any deviations from what is planned.

Implementation of registration systems and acquisition of legally required documentation and certifications

Relevant health and safety documentation is managed in paper and computer form (data base and company management programs) by the respective relevant company figures.

Surveillance and disciplinary system

The Employer, also through the persons in charge, must carry out supervisory activities on the application, including by employees, of the regulations and requirements regarding health and safety at work as well as carry out periodic control activities designed to verify the effectiveness of the procedures adopted and to ensure that the conditions of suitability of the measures adopted are maintained over time. The Employer must apply the appropriate disciplinary measures in case of non-compliant behavior with the aforementioned regulations and requirements.

There is a suitable disciplinary system in place regarding occupational health and safety, in line with the regulatory provisions of Article 30 of Legislative Decree 81/08 and consistent with the National Collective Agreement applied.

An information flow, concerning the disciplinary measures taken, to the RSPP is provided in order to enable appropriate risk control measures to be established, if necessary.

14.2. Environmental compliance management

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Waste Management • Energy control - local air conditioning (refrigerating equipment containing FGAS)	• Administrative Body • Office Coordinator • All workers (employees and contractors)	• Environmental crimes (Art. 25-undecies) - Environmental pollution - Waste management offenses - Organized activities for the illegal trafficking of waste

14.2.1. Specific principles of behavior

All employees and contractors of the Company must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the obligations under national and international environmental protection regulations as well as scrupulously observe the provisions and instructions issued by the Company in order to preserve the environment;
- Comply with the power of attorney system in place;
- Promptly report any situations of danger to the environment and violations of the rules of conduct defined in this Model;
- Carry out the collection and on-site temporary storage of urban, assimilable to urban and special wastes in accordance with the regulations and practices of good engineering and environmental prevention, properly classifying and characterizing them in the prescribed categories and hazard classes also ensuring the presence of markings indicating the correct containers;
- Supervise the conduct of the control of the volume and storage time of waste placed in temporary storage facilities so that the relevant legal requirements are met;
- To entrust municipal and assimilated waste to locally authorized Ad Hoc Services through appropriate agreement, for transportation and disposal within the terms of the law.

It is also expressly forbidden:

- Engage in conduct that may constitute an offense included among those considered by Legislative Decree 152/2006 or may become one.

Those who are specifically responsible at the Company's headquarters and offices located throughout the country for environmental compliance must also:

- define at the locations/offices suitable regulations also identifying precise precautionary rules to be followed in order to ensure the necessary environmental protection;
- Pursue the goal of "no harm to the environment." Cost and time-saving goals should not be pursued at the expense of environmental protection;
- Promote a culture in which all employees and contractors participate in this commitment;
- define, potential environmental risks in order to properly manage them;
- Ensure an adequate level of information to employees and collaborators on environmental protection and the consequences of non-compliance with legal regulations and the rules of behavior and control defined by the Company;
- Promptly report to the Office Coordinator any signs/events of risk/hazard to the environment regardless of their severity.

14.2.2. Specific control safeguards

The Company has adopted the following procedure for managing environmental compliance:

- PR09 "Environmental Aspects Management.

The aforementioned procedure, which is intended to govern environmental compliance relevant to LKIBS, can be found in the company's dedicated and shared information system.

In addition, under the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding aspects related to environmental issues.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

In light of this premise, compliance with all required and applicable environmental obligations, including the specific control safeguards below, must be ensured.

Waste Management

It should be noted that currently LKIBS does not directly dispose of special wastes (hazardous and non-hazardous), and all special wastes are entrusted to the third parties who generated them for subsequent management in accordance with current regulations.

Office Coordinator is responsible for following up on activities for waste disposal management, specifically:

- Contact the managing entity;
- Agrees on waste pickup;
- Verifies compliance with waste collection procedures by all personnel.

Should the specific occurrence of special waste disposal as a "Producer" arise, LKIBS shall:

- entrust special, hazardous and non-hazardous waste to authorized and registered transport, recovery and disposal companies, taking care to ascertain the existence of the *ex lege* requirements of the providers of waste disposal services (such as, by way of example, authorizations and registration with the National Register of Environmental Managers), acquiring a conformed hard copy of the relevant documentation, where it is not possible to obtain the original copy or through the official lists of the authorizing bodies;
- Conduct periodic reviews of the maintenance over time of the *ex lege* requirements of disposers verified at the selection stage;

- Verify the correctness of the data recorded in the annual waste declaration (MUD), if due according to the type of waste disposed in the reference year, before signing it and arranging for it to be sent to the relevant bodies;
- periodically ensure that the fourth copy of the Waste Identification Form has been received within the legal deadlines;
- Ensure that the Company's contracted suppliers use waste analysis certificates containing correct and truthful information on the nature, composition and chemical and physical characteristics of the transported waste.

Energy management - local air conditioning

The air conditioning of the premises is provided by systems that are regularly checked and comply with current environmental protection laws.

Office Coordinator is responsible for ensuring necessary checks and maintenance.

In the case of locations at office centers, compatibility with environmental standards is ensured by the supplier, selected according to supplier selection procedures.

Where equipment containing FGAS in quantities greater than 5t CO2 equivalent is installed, maintenance managers shall, if contractually responsible:

- subject systems containing refrigerant gases (fluorinated greenhouse gases - FGAS) to periodic maintenance by specialized personnel (carefully selected according to the necessary legislative requirements) in order to ensure their efficiency and periodic leak testing of refrigerant circuits to preserve the environment from leakage;
- Correctly file and periodically update the license plate data, the amount of FGAS contained, and information on maintenance performed by receiving feedback from FGAS operators of the correct uploading of data into the Fluorinated Gas Database.

14.3. Managing relationships with private certifying bodies

Related activities (illustrative)	Main Contacts/Organizational Units Involved.	Associable offenses under Legislative Decree 231/01 (see Appendix 1 for details)
• Management of relations with representatives of certifying bodies in the course of audits carried out by them both when issuing certifications and in subsequent renewals of certifications	• Administrative Body • Compliance and Quality	• Corporate crimes (Art. 25-ter) - Bribery among private individuals - Incitement to bribery among private individuals

14.3.1. Specific principles of behavior

Those who, by reason of their position or function, are involved in the sensitive activity must:

- Comply with applicable laws and the principles set forth in the company's Code of Ethics and this Model;
- Comply with the power of attorney system in place;
- Maintain fair, transparent, documented, verifiable, impartial and cooperative relationships with representatives of certifying bodies;
- report, without delay, to their hierarchical manager any attempts of undue requests by representatives of the certifying bodies, aimed, for example, at obtaining favors, illicit handouts of money or other benefits, including to third parties, as well as any critical issues arising within the relationship with them;
- provide, to its employees and collaborators adequate directives on how to conduct themselves in formal and informal contacts with representatives of accredited certifying bodies;
- Give full and immediate cooperation to representatives of accredited certifying bodies during inspections, providing the requested documentation and information in a timely and comprehensive manner.

It is also expressly forbidden:

- Pay or offer, directly or indirectly, including in different forms of aid or contributions, payments or material benefits to the counterparty or persons close to them, in order to influence their behavior and ensure advantages of any kind to the Company;
- give in to improper recommendations or pressure from representatives of certifying bodies.

14.3.2. Specific control safeguards

Those who, by reason of their position or function, are involved in the sensitive activity must ensure the control safeguards below.

On the heads of the Organizational Units identified by corporate procedure PR14 "Information flows and attestations to the Supervisory Board" there is also an obligation to transmit to the Board, on a periodic or event-driven basis, any information required by the procedure itself regarding relations with certifying bodies.

Company procedures can be found on the company's computerized dashboard, and all LKIBS personnel are required to comply with them.

- Relations with certifying bodies are handled exclusively by Compliance and Quality under the coordination of the Administrative Body.
- Only accredited entities may be selected for the purpose of obtaining or renewing certifications.
- Relationships with certifying bodies must be governed by appropriate contracts authorized and signed by individuals with appropriate powers.
- At least two company representatives shall be present at the audits conducted by representatives of the certifying bodies, and they shall ensure that the audits are carried out properly, making available all the documentation and information required and necessary for the performance of the activity.
- Meetings held with representatives of certifying bodies, at the close of audit or annual activities, must be documented by appropriate minutes shared with the Administrative Body.
- Approval for payment of the invoice to the certifying body should be granted, where possible, prior to any issuance/renewal of certification.
- All relevant documentation under this sensitive activity is archived by Compliance and Quality.