

**ORGANISATION, MANAGEMENT AND CONTROL MODEL**

***Adopted pursuant to Italian Legislative Decree no. 231/2001***

**GENERAL PART - SPECIAL PART**

**S.C.F S.r.l**

***Approved by the Board of Directors on 21 March 2024***

## Contents

<b>Definitions .....</b>	<b>4</b>
<b>Document structure .....</b>	<b>6</b>
<b>General Part.....</b>	<b>7</b>
1. Legislative Decree no. 231 of 8 June 2001 .....	8
1.1. Characteristics and nature of liability of entities.....	8
1.2. Types of crime identified by the Decree and subsequent amendments .....	9
1.3. Criteria for attributing liability to an entity .....	11
1.4. Indications of the Decree regarding the characteristics of the Organisation, Management and Control Model .....	14
1.5. Crimes committed abroad .....	15
1.6. The sanctions .....	15
1.7. Changes in the entity .....	18
2. Aims of the Model .....	19
3. Model and Code of Ethics .....	19
6. Adoption of the Model by S.C.F. ....	22
In compliance with the provisions of the Decree, the Company adopts its own Organisation, Management and Control Model. ....	22
Both the adoption and any subsequent changes of this document are the exclusive responsibility of the Board of Directors.....	22
7. Relevant crimes for S.C.F. ....	23
8. Recipients of the Model.....	36
9. Supervisory Body .....	37
9.1. Function .....	37
9.2. Appointment of the members of the Supervisory Body .....	38
9.3. Eligibility Requirements. Forfeiture and replacement. ....	39
9.4. Dismissal and withdrawal .....	39
9.5. Powers .....	40
9.6. Information flows to and from the Supervisory Body .....	42
10. Provision of goods or services by consortia and/or other companies .....	44
11. Communication and training.....	45
<b>Special Part .....</b>	<b>46</b>
2. General principles of conduct .....	47
3. General prevention protocols .....	47
A. Crimes against Public Administration .....	50
A1. Sensitive activities in the context of crimes against the Public Administration .....	51
A2. Specific prevention protocols .....	52
B. Cybercrimes.....	57
B1. Sensitive activities in the context of cybercrimes .....	57
B2. Specific prevention protocols .....	57
C. Corporate crimes.....	58
C1. Sensitive activities in the context of corporate crimes.....	58
C2. Specific prevention protocols .....	59
D. Involuntary manslaughter and serious and very serious injuries due to negligence, committed in breach of accident prevention regulations and regulations relating to the protection of hygiene and health at work .....	62
D1. Premise .....	62
D2. Sensitive activities in the context of the crimes of involuntary manslaughter and serious and very serious injuries due to negligence, committed in breach of accident prevention regulations and regulations relating to the protection of hygiene and health at work.....	65
D2.1 Activities at risk of injury and occupational disease .....	66
D2.2 Activities at risk of crime .....	66
F.1 General principles of conduct .....	68
D4. General prevention protocols .....	70
D5. Specific prevention protocols .....	71

D6.	Further prevention protocols.....	80
E.	Receiving stolen goods, laundering, use of money, goods or benefits of illicit origin and self-laundering; crimes relating to payment instruments other than cash and fraudulent transfer of values .....	81
E1.	Sensitive activities in the context of crimes of receiving stolen goods, laundering, use of money, goods or benefits of illicit origin and self-laundering .....	81
E2.	Specific prevention protocols .....	81
F.	Crimes relating to copyright infringement .....	83
G.	Inducement not to make statements or to make false statements to the Judicial Authority .....	84
H.	Employment of third-country nationals whose stay is irregular .....	85
I.	Racism and xenophobia crimes.....	85
J.	Tax crimes.....	86

## **Definitions**

- **Sensitive activities:** these are activities carried out by S.C.F. which entail the risk, even potential, of the crimes referred to in Legislative Decree no. 231/2001 being committed.
- **Company:** S.C.F. S.r.l., also referred to as S.C.F.
- **Consultants:** professionally qualified persons who render professional service to or on behalf of S.C.F.
- **Legislative Decree no. 231/01 or the Decree:** Italian Legislative Decree no. 231 of 8 June 2001 and subsequent amendments or additions.
- **Employees:** persons having a subordinate or quasi-subordinate employment contract with S.C.F.
- **Public service officer:** A person who *“in any capacity, provides a public service”, i.e., performs "an activity governed in the same way as a public function but characterised by the lack of the powers that are typical of the latter, excluding simple executive tasks and the provision of merely material work"* (Criminal Code, Art. 358).
- **Confindustria Guidelines:** This is the document (approved on 7 March 2002 and subsequently updated, latest update in June 2021) containing guidelines from Confindustria for building the organisation, management and control models referred to in the Decree.
- **Model:** Organisation, management and control model pursuant to Legislative Decree no. 231/01.
- **Consortium bodies:** These are both the Board of Directors and the Board of Auditors of S.C.F.
- **Supervisory Body or SB:** The body provided for by Art. 9 of the Decree, responsible for supervising the functioning of the Model and compliance with it.
- **P.A.:** This acronym refers to both Public Administration intended as an entity, office or body, and a natural person invested, even de-facto, with the correspondent functions, i.e., a public official or a public service officer.
- **Partners:** these are contractual counterparties to S.C.F., i.e., natural or legal persons with whom S.C.F. establishes a collaboration relation regulated by a contract.

- **Public official:** a person who "exercises [even de-facto] a public legislative, judicial or administrative function" (Criminal Code, Art. 357).
- **Personnel manager:** a person responsible for the training of personnel, with particular attention, in this context, to the principles and contents set out in Legislative Decree no. 231/2001. Unless otherwise specified, this role is covered by the General Manager.
- **Internal Manager:** a person vested with responsibilities relevant to all operations that concern sensitive activities and are considered risky, according to Legislative Decree no. 231/2001. Unless otherwise specified, this role is covered by the General Manager.
- **Crimes:** these are the types of crime to which the provisions set out in Legislative Decree no. 231/01, and subsequent amendments or additions apply.
- **Top managers:** persons holding representation, administrative or directive roles in the Company or in one of its units with financial and functional autonomy, and persons managing or controlling the Company, even de-facto.
- **Subordinates:** persons subject to the direction or supervision of one of the persons referred to in the previous point.
- **CSA:** Italian Legislative Decree no. 81 of 09 April 2008, also known as 'Testo unico sulla sicurezza' (Consolidated safety act) and subsequent additions and/or modifications.

## **Document structure**

This document, made up of a General Part and a Special Part, includes consideration of the provisions of Legislative Decree no. 231/01 (hereinafter also referred to as the '**Decree**') and sets out the guidelines that describe the process implemented by S.C.F. (hereinafter also referred to as the '**Company**'), for adopting the Model, the crimes that the Model considers relevant, the recipients of the Model, the Supervisory Body (hereinafter also referred to as '**SB**'), the obligations to communicate the Model and train personnel.

The second part indicates the sensitive activities for the Company pursuant to the Decree, i.e. those at risk of crime, the general principles of conduct, the prevention elements to protect the aforementioned activities and the essential control measures designed to prevent or mitigate the crimes.

In addition to that which is expressly established below, the following are also an integral part of this document:

- **The Code of Ethics**, defining the principles and rules of corporate conduct.
- **The Procedures Manual**, containing specific risk prevention protocols
- **The Disciplinary System**, which guarantees compliance with the Organisational Model, according to the combined provisions of Article 6, paragraph 2, letter e) of the Decree.
- All Company's provisions, internal measures, deeds and operating procedures that constitute implementation of this document. The said deeds and documents are made available according to the methods established for their dissemination within the Company.

## **General Part**

## **1. Legislative Decree no. 231 of 8 June 2001**

The Decree, which introduces and regulates administrative liability arising from crimes committed by entities, incorporates and implements European Community legislation on the fight against corruption, creating a unicum in the Italian legal system, which until 2001 did not provide for any form of criminal or administrative liability for collective entities, who, at most, could be called upon to jointly and severally pay fines for crimes committed by their legal representatives.

The scope of the Decree is very broad and concerns all entities with legal personality, companies, associations, even without legal personality, public economic entities, private entities providing public services, the State excluded, public territorial entities, public non-economic entities, and entities that perform functions of constitutional importance (e.g., political parties and trade unions).

The Decree does not mention entities having their registered offices outside of Italy. However, on this point we should mention an order (dated 13.06.2007) in which the Preliminary Investigation Judge of the Court of Milan affirmed that, based on the territoriality principle, Italian judges have jurisdiction on crimes committed by foreign entities in Italy.

### **1.1. Characteristics and nature of liability of entities**

The Law-maker has identified different types of crimes, committed by natural persons, that can be committed in the interest or to the advantage of a company: after having identified the link between the entity and the perpetrator of the crime, and having ascertained that the latter acted within the scope of its business, the Decree considers the dual concepts 'natural person - entity' and 'crime - interest of the entity' and from them infers a direct liability of the latter, and chooses a particular punitive system that is independent from and parallel to that applicable to a natural person.

This new form of entity's liability is mixed, as it combines the essential features of the criminal and administrative law systems.

Indeed:



1. The entity is punished with an administrative sanction, answering for an administrative offence.
2. The sanctioning system is based on criminal proceedings, as the authority responsible for charging an entity with a crime is the Public Prosecutor, while the criminal judge is responsible for imposing the sanction.

The administrative liability of the entity is distinct and autonomous from that of the natural person who commits the crime, and arises even in the absence of identification of the perpetrator of the crime, or in the event that the crime is extinguished for a reason other than amnesty.

**In any case, the liability of the entity is always added to, and never replaces, that of the natural person who committed the crime.**

## **1.2. Types of crime identified by the Decree and subsequent amendments**

In compliance with the typicality principles that informs our criminal law system, an entity can be called to answer for a limited number of crimes, i.e., only for those crimes expressly indicated by the Law-maker and committed in the interest or to the advantage of the entity, excluding any other type of crime committed by top managers or subordinates during the life of a company. Articles 24 and following of the Decree, in its original version and subsequent additions, as well as the laws that expressly refer to the discipline at issue, list the crimes that may give rise to the liability of the entity, which are called **predicate crimes**.

The limit represented by the principle of typicality, combined with the actual prospect of an interest or advantage for the entity, is justified by the fact that it would be illogical to punish the entity for crimes that have no connection whatsoever with its own business activity but are instead attributable to the personal choices made by the individual who commits them. Predicate crimes include very different types of crime, some of which are characteristic of business activities while other are specific to criminal organisations.

As of the date of approval of this document, the predicate crimes belong to the categories indicated below:

- a. Crimes committed in relations with the Public Administration bodies (Articles 24 and 25).

- b. Crimes of forgery of money, public credit cards and stamps and instruments or signs of recognition (Art. 25-bis).
- c. Crimes against industry and trade (Art. 25-bis.1).
- d. Corporate crimes (Art. 25-ter), among which the most notable is private corruption (Civil Code, Art. 2635, para. 3, also in the form of instigation pursuant to Civil Code, Art. 2635-bis).
- e. Crimes for purposes of terrorism or subversion of the democratic order, provided for by the Criminal Code or by special laws; crimes committed in violation of the provisions of Art. 2 of the International Convention for the Suppression of the Financing of Terrorism, issued in New York on 9.12.1999 (Art. 25-quater).
- f. Female genital mutilation practices (Art.25-quater.1).
- g. Crimes against the individual personality (Art. 25-quinquies).
- h. Market abuse (Art. 25-sexies).
- i. Involuntary manslaughter and serious or very serious negligent personal injury, committed in violation of the occupational accident prevention and occupational health and hygiene regulations (Art. 25-septies).
- j. Transnational crimes (Law 146/2006, Art. 10).
- k. Receiving, laundering and use of money, assets or benefits of illicit origin and self-laundering (Art. 25-octies).
- l. Offences or crimes relating to non-cash payment instruments and fraudulent transfer of assets (Art. 25-octies.1)
- m. Copyright infringement crimes (25- nonies).
- n. Inducement not to make statements or to make false statements to a judicial authority (Art. 25-decies).
- o. Environmental crimes (Art. 25-undecies).
- p. Employment of third-country nationals whose stay is irregular (Art. 25-duodecies).
- q. Computer crimes and unlawful data processing (Art. 24-bis).
- r. Organised crime offences (Art. 24-ter).

- s. Racism and xenophobia crimes (Art. 25-terdecies)
- t. Fraud in sports competition, illegal gambling or betting and gambling games carried out by means of prohibited devices
- u. Tax crimes (Art. 25-quinquiesdecies)
- v. Smuggling crimes (Art. 25-sexiesdecies)
- w. Crimes against cultural heritage (Art. 25-septiesdecies)
- x. Laundering of cultural assets and devastation and looting of cultural and landscape assets (Art. 25-duodevices)

The applicability and relevance of each crime for S.C.F. will be discussed in-depth in section 7 of this General Part.

### 1.3. Criteria for attributing liability to an entity

In the event of the commission of a predicate crime, the entity is punishable only if certain conditions are met; these conditions are the **‘criteria for attribution’** of a crime to the entity.

These criteria are divided into objective and subjective criteria.

The first objective condition is that the crime was committed by a person linked to the entity by a qualified relation. It follows, in essence, that there must be a relevant connection between the perpetrator of the crime and the entity, with administrative liability on the part of the latter if the offender belongs to one of the following categories:

- Top managers, such as, or example, the legal representative, the director, the general manager or the manager of an autonomous organizational unit, as well as the persons who manage the entity, even if only de facto. These are the persons who actually have the power to make decisions in the name and on behalf of the Company. In addition, all the persons mandated by directors to manage or direct the activity of the entity or its branches, are considered as part of this category.
- Subordinate persons, i.e., all those who are subject to the direction and supervision of the top management. Specifically, this category includes employees and those individuals who, although not being part of personnel, have tasks to perform under the direction and control of the top management. On this point, it should be noted that case law gives particular

importance to the activity actually carried out rather than to the existence of a subordinate employment contract, in order to prevent the entity from circumventing law by mandating external parties activities that could constitute crimes. These external parties include, inter alia, collaborators, promoters, agents and consultants mandated by the entity to carry out activities on its behalf. Finally, legally relevant are also agency or contractual relations with individuals who are not part of the company's personnel, provided that they operate in the name, on behalf or in the interest of the entity.

The second objective condition is that the crime was committed in the interest or to the advantage of the entity. This means that it must have been committed in an area inherent to the specific activities of the entity, and the latter must have obtained a benefit from it, even if only potential.

The existence of at least one of the two alternative conditions is sufficient:

- There is interest when the perpetrator of the crime has acted with the intent of benefiting the entity, regardless of whether this objective was actually achieved.
- There is advantage when the company has obtained, or could have obtained, a positive result, financial or otherwise, from the crime.

According to the Court of Cassation (Cass. Pen., no. 3615/06), the concepts of interest and advantage should not be understood as a unit but as separate concepts, since the conceptual distinction between a possible gain envisaged as a consequence of the illicit act, compared to an advantage actually obtained thanks to the crime, is clear. The Court of Milan also ruled accordingly (order of 20 December 2004), stating that, for the requirement in question, the sole fact that the criminal conduct was aimed to the pursuit of a given benefit is sufficient, regardless of whether it has actually been achieved.

In other words, the liability of the entity exists not only when it has derived an immediate financial advantage from the commission of the crime, but also when, even in the absence of such a result, the crime is motivated by the interest of the company: the improvement of its position on the market or the concealment of a situation of financial crisis are cases that involve the interests of the company without bringing it an immediate financial or economic advantage.

The conditions under which the crime is attributable to the entity are established by subjective criteria of attribution: the crime is not attributable to the entity where, before its occurrence, the entity has equipped itself with an Organisation, Management and Control Model suitable for preventing crimes of the type that was committed. In essence, in order for the crime not to be attributed to the entity, the latter must demonstrate that it has done everything possible to prevent, within the scope of the exercise of its business activity, the commission of one of the crimes provided for by the Decree.

On this point, Legislative Decree 231/2001 provides for the exclusion of liability only if the entity demonstrates that:

- Before the crime was committed, the governing body adopted and effectively implemented an organisation, management and control model suitable for preventing crimes of the type that occurred.
- The task of supervising the functioning and observance of the model and ensuring their updating has been entrusted to a body within the entity that has autonomous powers of initiative and control.
- There was no omission or insufficient supervision by the aforementioned body, which must be equipped with autonomous powers of initiative and control.

In order to exclude the liability of the entity, all conditions listed above must be met at the same time: therefore, exemption from liability derives from the adoption and effective implementation of a crime prevention model, and from the simultaneous establishment of a Supervisory Body, which is assigned the task of monitoring the compliance of the activity carried out within the company with respect to the standards and procedures established in the Model.

The Decree is much more rigid and severe in the case in which the crime is committed by a top manager, even though the model acts as a cause of non-liability in the case of both a predicate crime committed by a top manager, and of a crime committed by a subordinate. In the first case, since the entity must demonstrate that the perpetrator committed the crime by fraudulently eluding the model, the Decree requires stronger proof of non-involvement, as the entity is required to prove a sort of internal fraud by the top manager.

Conversely, in the event of crimes committed by persons in a subordinate position, the entity may be held liable only if it is ascertained that committing the crime was made possible by failure to comply with management or supervisory obligations. In this case, it is a real organisational fault, as the entity indirectly consented to the commission of the crime by not supervising the activities and the individuals that were at risk of committing a predicate crime.

The law does not mandatorily require entities to equip themselves with a 231 model; however, based on the criteria for attributing crimes to entities, the 231 model seems to be the only tool capable of demonstrating an entity's non-involvement and preventing the application of the sanctions established by the Decree.

Therefore, equipping itself with an effective and efficient model is in the interest of the entity.

#### **1.4. Indications of the Decree regarding the characteristics of the Organisation, Management and Control Model**

The mere adoption of the Model is not the sole and sufficient condition to exclude the liability of a company, since the Decree limits itself to regulating some general principles, without specifying their characteristics.

The Model operates as a cause of non-liability only if it is:

- **Effective**, i.e., reasonably suitable to prevent the crime or crimes committed.
- **Actually implemented**, i.e., its content is applied in corporate procedures and the internal control system.

As for the effectiveness of the model, the Decree establishes its minimum content, as follows:

- a. **Identification of the company's activities carried which entail the risk of crimes to be committed.**
- b. **Drafting of specific protocols aimed at planning the formation and implementation of the entity's decisions on the crimes to be prevented, also through the implementation of written procedures that are additional and/or pre-existing to the Model.**

- c. Identifying financial resource management methods that are suitable for preventing the commission of crimes.
- d. Introducing a disciplinary system for sanctioning failure to comply with the measures indicated in the model.
- e. Providing for information obligations towards the Supervisory Body.
- f. Providing for suitable measures to ensure that the activity is carried out in compliance with the law, risk situations are promptly detected and eliminated that are linked to the nature and size of the organisation and the type of activity it carries out.

The Decree establishes that the model be subject to periodic verification and updating, both in the case significant violations of the provisions are discovered, and in the case significant changes occur in the company's organisation or activity.

The model, although varying and adapting to the nature, size and specific activities of the company, can be configured as a set of principles, tools and conduct that regulate the organisation and management of the company as well as its control tools.

### **1.5. Crimes committed abroad**

Pursuant to Article 4 of the Decree, the entity may be held liable in Italy for predicate crimes committed abroad.

However, the Decree subjects this possibility to the following conditions:

- The State of the place where a crime was committed is not taking relevant proceedings.
- The company has its headquarters in the territory of the Italian State.
- The crime is committed abroad by a person functionally linked to the company.
- The general conditions for admissibility exist under Articles 7, 8, 9, 10 of the Criminal Code.

### **1.6. The sanctions**

When held liable, the entity can be sentenced to four types of sanctions, different in nature and method of execution:

1) Pecuniary sanction.

A pecuniary sanction is applied whenever the judge deems the entity liable. The sanction depends on a system of 'shares' determined by the judge. The amount of the pecuniary sanction depends on the seriousness of the crime, the entity's degree of liability, the activity carried out to eliminate or mitigate the consequences of the crime or prevent the commission of similar crimes. The judge, in determining the amount, also takes into account the financial conditions and assets of the entity.

2) Disqualification sanction.

Disqualification sanctions may be applied in addition to pecuniary sanctions only if expressly provided for the crime being prosecuted and only if at least one of the following conditions occurs:

- The entity has derived a significant profit from the crime and the crime was committed by a person in a managerial position, or by a subordinate person, when the commission of the crime was made possible by serious organisational deficiencies.
- In case of repetition of the offences or crimes.

The disqualification sanctions provided for by the Decree are:

- Temporary or permanent suspension from carrying out the activity.
- Suspension or revocation of authorisations, licenses or concessions that were functional to the commission of the crime.
- Prohibition on contracting with Public Administration bodies, except to obtain the provision of a public service.
- Exclusion from benefits, financing, contributions or subsidies and any revocation of those already granted..
- Temporary or permanent ban on advertising goods or services.

Disqualification sanctions are applied with definitive effects only in exceptional cases, as they are usually temporary, from three months to one year, and their object is the specific activity involved in the entity's crime. Disqualification sanctions may also be applied as a precautionary measure, before the conviction, at the request of the Public Prosecutor, where there are serious indications regarding the liability of the entity and there are well-founded



and specific elements that lead to the belief that there is a concrete risk that illicit acts of the same type as those being prosecuted will be committed.

### 3) Confiscation.

It is the acquisition by the State of the price or profit of the crime or of an equivalent value. Profit of the crime means the financial advantage that derives from the crime, with this financial advantage to be understood not as net profit or income but rather as an additional benefit in terms of patrimonial assets. Moreover, according to the Court of Naples (order of 26 July 2007), the lack of a decrease in patrimonial assets following non-disbursement of money for costs that should have been borne, is not extraneous to the concept of profit; this although recently (Cass. Pen., VI, 20.12.2013, no. 3635) it has been stated that *“With regard to the criminal liability of entities, the profit of the crime is identified with the positive financial advantage that has the predicate crime as its direct and immediate cause. This advantage may also consist of a saving in expenditure, which is, however, to be understood in a relative sense, i.e., as revenue received from which the costs that should have been sustained have not been deducted, and is not to be understood in an absolute sense, i.e., as a decrease or lack of increase in liabilities which do not correspond to assets of which the liable party has materially become the owner”*.

### 4) Publication of the conviction sentence.

The conviction sentence is published only once, as an extract or full text, at the expense of the entity, in one or more journals as indicated by the judge in the sentence as well as by posting it at the Municipality where the entity has its headquarters.

Although applied by the criminal judge, all sanctions are of an administrative nature: the framework described above is very severe, both due to the high sums of pecuniary sanctions and because the disqualification sanctions can significantly limit the exercise of normal business activity, precluding a series of businesses.

Administrative sanctions against the entity expire at five years from the date the crime was committed.

The final conviction of the entity is entered in the national register of administrative sanctions for crimes, which is an archive containing all decisions relating to sanctions that have become irrevocable and have been applied to entities pursuant to the Decree.

### **1.7. Changes in the entity**

The Decree also regulates the liability regime of the entity in the event of changes such as company transformation, merger, split or transfer.

The fundamental principle establishes that the obligation to pay pecuniary sanctions is solely on the entity, which may pay using its assets or common fund. Therefore, regardless of the legal nature of the collective entity, shareholders or associates are not directly liable with their assets.

The principles of civil law on the liability of the entity undergoing transformation for the debts of the original entity are applied, as a general criterion, to the pecuniary sanctions imposed on the entity. However, disqualification sanctions remain the responsibility of the entity in which the business branch in which the crime was committed has remained (or has merged).

In the event of transformation of the entity, liability for crimes committed prior to the date on which the transformation took effect remains in place: the new entity will therefore be subject to the sanctions applicable to the original entity for acts committed prior to the transformation.

In the event of a merger, the entity resulting from the merger, including by incorporation, shall be liable for the crimes for which the entities participating in the operation were liable. If the merger occurred before concluding the judgement of liability of the entity, the judge shall take into account the financial conditions of the original entity and not those of the entity resulting from the merger.

In the event of transfer or assignment of the company within which the crime was committed, without prejudice to the benefit of first suing the transferring entity, the transferee is jointly and severally liable with the transferor to pay the pecuniary sanction, within the limits of the value of the transferred company and within the limits of the pecuniary sanctions that result from the mandatory accounting books, or of which the transferee was in any case aware. In any case, the disqualification sanctions apply to entities to which the business branch in which the crime was committed has remained or has been, even in part, transferred.

## **2. Aims of the Model**

By adopting this Model, S.C.F. intends to promptly comply with the legislation on the criminal-administrative liability of legal persons, conform to the inspiring principles of the Decree, improve and make its existing internal controls and corporate governance systems as efficient as possible.

The main objective of the Model is to create an organic and structured system of control principles and procedures suitable to prevent, where possible and practically feasible, the commission of the crimes provided for by the Decree. The Model shall be embedded in the company's own governance system and a corporate culture based on correctness, transparency and legality shall be promoted.

The Model also aims to achieve the following aims:

- Providing adequate information to employees and persons acting on behalf of the Company, or linked to it by relations that are relevant under the Decree, regarding activities that involve the risk of committing crimes.
- Spreading a corporate culture based on legality, as the Company condemns any conduct that does not comply with the law or internal provisions, and in particular the provisions contained in its Organisational Model.
- Spreading a culture of control.
- Implementing an effective and efficient corporate organisation, placing particular emphasis on the decision-making process and its transparency, the provision of preventive and subsequent controls, as well as the management of internal and external information.
- Implementing all necessary measures to eliminate as quickly as possible any situations where crimes could be committed.

## **3. Model and Code of Ethics**

The Company adopts its own Code of Ethics, approved by resolution of the Board of Directors dated 27/06/2012.

The ultimate goal of the Code of Ethics is to establish the rules of conduct and the ethical and social values that S.C.F. must be imbued with while pursuing of its consortium purpose and objectives, in compliance with that which is reported in this document.

The Model implies compliance with the provisions of the Code of Ethics, and forms a single body of rules with it, aimed at spreading a culture based on ethics and corporate transparency.

The Company's Code of Ethics, which is hereby fully referred to, constitutes the essential foundation of the Model and the provisions contained in the Model are an addition to that which is established by the Code of Ethics.

#### **4. Changes and updates to the Model**

This document must always be promptly modified or integrated, by resolution of the Board of Directors, also upon proposal from the Supervisory Body, and in any case always after having heard the Supervisory Body, when:

- Violations or evasions of the provisions of this Model have occurred that have shown the ineffectiveness or inconsistency of the Model in preventing crimes.
- Significant changes have occurred in the regulatory framework, organisation or business of the Company.
- In all other cases where it is necessary or useful to make changes to the Model.

#### **5. S.C.F.: the Company.**

S.C.F. has as its business purpose the mutual management, in Italy and abroad and excluding any profit-making purpose, of a series of rights that are detailed in the Company's instrument of incorporation and articles of association, documents that are considered an integral part of this Code. The said rights also include, by way of example and not limited to, the right to remuneration and fair remuneration for the use, either for profit or not, of phonograms by means of radio and television broadcasting at public dance parties, in shops and on the occasion of any other public use of the phonograms, pursuant to Articles 73 and 73-bis of Law 633 of 22.04.1941 and subsequent amendments, and also include the right to remuneration for

private reproduction for personal use, pursuant to Art. 71-septies of Law 633 of 22.04.1941 and subsequent amendments.

As of the date of approval of the new Articles of Association (04.29.2014), the Company's corporate governance system is structured as follows:

- General meeting:

The General Meeting is competent to deliberate, in ordinary and extraordinary sessions, on matters reserved to it by law or the Articles of Association.

- Board of Directors:

The Board of Directors is invested with the broadest powers of ordinary and extraordinary administration of the Company, and has the authority to carry out all acts deemed useful and appropriate for achieving the consortium purposes.

The Chairman of the Board of Directors shall chair general meetings and meetings of the Board of Directors, has the legal representation of the Company before third parties and in court, and may also issue special powers of attorney. In the event of his/her absence or impediment, the Vice-Presidents shall act, even disjunctly.

- Advisory Committee:

The Advisory Committee issues non-binding opinions upon request of the Board of Directors.

- Board of Auditors:

The Board of Auditors, composed of three effective auditors and two substitutes, supervises compliance with the law and the Articles of Association, compliance with the principles of correct management and, in particular, the adequacy of the organisational, management and accounting structure adopted by the Company and its correct functioning.

- Statutory Auditing Firm:

The ordinary meeting appoints a statutory auditing firm, registered in the specific register referred to in the Legislative Decree no. 39 of 27.01.2010, appointing it to perform the functions referred to in the Civil Code, Articles 2409-bis and following article (i.e., statutory auditing of accounts and performance of accounting control functions).

- Scientific Advisory Board:

The Board of Directors may decide to establish a Scientific Advisory Board, tasked with providing high-level advice in matters of intellectual property law, business law, profit-making and non-profit associations, bond and contract law and any other matter connected to those listed above.

## **6. Adoption of the Model by S.C.F.**

In compliance with the provisions of the Decree, the Company adopts its own Organisation, Management and Control Model.

Both the adoption and any subsequent changes of this document are the exclusive responsibility of the Board of Directors.

The Model, inspired by the Guidelines on Legislative Decree no. 231 of 8 June 2001, proposed by Confindustria, in their latest version as of 2021, was drawn up taking into account the structure and the business activity actually carried out by the Company and the nature and size of its organisation.

The Company analysed its business context and the areas of activity that entail a potential risky for the crimes indicated by the Decree to be committed; lastly, it analysed its existing procedures for carrying out operations.

Therefore, for the preparing this document, the Company:

- Identified sensitive activities, i.e., areas in which the predicate crimes indicated in the Decree may be committed, through interviews with the heads of company functions.
- Performed a control and risk self assessment regarding potential commission of crimes and its internal control system suitable for intercepting any illicit conduct.
- Identified proper control measures, existing or to be implemented, necessary for preventing the crimes referred to in the Decree or mitigating the risk for crimes to be committed.
- Reviewed its system of delegations and powers and attribution of responsibilities.

Regarding the possible commission of crimes against the person (Art. 25-septies of the Decree), the Company analysed its business context and all the specific activities carried out therein, and assessed the risks connected thereto on the basis of the findings of the checks

carried out in compliance with the provisions of Legislative Decree no. 81 of 9 April 2008 and the special legislation connected to it.

This document constitutes the internal regulations of the Company and is binding on the Company.

## 7. Relevant crimes for S.C.F.

The Model for S.C.F. was developed taking into account the structure and activities actually carried out by the Company, as well as the nature and size of its organisation.

Taking into account these parameters, the Company has considered the following predicate crimes as relevant: Art. 24, 25 (Crimes against Public Administration), 24-bis (Computer crimes), 25-ter (Corporate Crimes), 25-septies (Involuntary manslaughter and serious or very serious negligent injury, committed in violation of occupational accident prevention and occupational health and hygiene regulations), 25-octies (Receiving, money laundering, use of money, assets or benefits of illicit origin and self-laundering), 25-octies.1 (Crimes relating to non-cash payment instruments and fraudulent transfer of assets); 25-nonies (Copyright infringement crimes), 25-decies (Inducement not to make statements or to make false statements to a judicial authority), 25-duodecies (employment of third-country nationals whose stay is irregular) 25-terdecies (racism and xenophobia), 25-quinquiesdecies (tax crimes).

In particular, within each category, the following crimes are currently considered applicable:

### A. Crimes committed in relations with the Public Administration bodies (Articles 24 and 25)

- ***Embezzlement of public funds***, provided for by Art. 316-bis of the Criminal Code. This crime consists in a party that is not part of the Public Administration, not allocating contributions, subsidies or funds obtained from the State or other public bodies or European Communities specifically for initiatives aimed at the realisation of works or the performance of activities of public interest, to these intended purposes.
- ***Undue receipt of public funds***, provided for by Art. 316-ter of the Criminal Code. This crime consists in unduly obtaining, for oneself or others, by using or making false statements or producing false documents or documents stating fact that are not true, or omitting information that must be provided, contributions, funds, subsidized loans or other disbursements of the same type, regardless of their name, that are granted or disbursed by the State, other public bodies or European Communities; this is unless the said conduct constitutes the crime provided for by Article 640-bis of the Criminal Code.

- **Fraud against the State or another public body**, provided for by the Criminal Code, Art. 640, para. 2, no. 1. This crime consists in a party obtaining an unjust profit for him/herself or others to the detriment of other parties, through artifice or deception or by inducing another party into error; this is when the said unjust profit is obtained to the detriment of the State or another public body or the European Union or under the pretext of exempting someone from military service.
- **Aggravated fraud for obtaining public funds**, provided for by Art. 640-bis of the Criminal Code. This crime consists in the same conduct as described in the previous point, when it is implemented to obtain contributions, funds, subsidized loans or other disbursements of the same type, regardless of their name, from the State, other public bodies or European Communities.
- **Computer fraud**, provided for by Art. 640-ter of the Criminal Code. This crime consists in altering in any way the functioning of a computer or telematic system or intervening with no authorisation and in any manner on data, information or software contained in or related to a computer or telematic system, in order to obtain, for oneself or others, an unjust profit to the detriment of the State or another public body.
- **Corruption in the exercise of one's own function**, provided for by Art. 318 of the Criminal Code. This crime consists in a public official receiving or accepting the promise of money or other benefits he/she is not entitled to for performing an act that is part of his/her official duties.
- **Instigation to corruption**, provided for by Art. 322 of the Criminal Code. This crime consists in offering or promising money or other undue benefits to a public official or a public service officer who holds the status of public servant, to induce him/her to perform an act that is part of his/her official duties, provided that the offer or promise is not accepted.
- **Corruption for an act contrary to official duties**, provided for by Art. 319 of the Criminal Code. This crime consists in a public official receiving or accepting the promise, for him/herself or for a third party, of money or other benefits for omitting or delaying or having omitted or delayed an act that is part of his/her official duties or to perform or to have performed an act that is contrary to his/her official duties.  
Following legislative changes introduced by Law no. 190 of 6 November 2012, the penalty imposed on the legal person is increased, in terms of the number of shares, where the crime referred to in Article 319 has as its object the assignment of public jobs or salaries or pensions or the conclusion of contracts involving the Public Administration body to which the public official concerned belongs, or tax payment or refund (Criminal Code, Art. 319-bis).
- **Corruption in judicial acts**, provided for by the Criminal Code, Art. 319-ter. This crime consists in facts of corruption committed to favour or damage a party in civil, criminal or administrative proceeding.
- **Undue inducement to give or promise benefits**, introduced by Law no. 190 of 6 November 2012. This crime consists in a public official or public service officer abusing his/her position or powers in order to induce someone to unduly give or promise him/her money or other benefits; this is unless this conduct constitutes a more serious crime. In the cases described above, whoever gives or promises money or other benefits is in turn punished (Criminal Code, Art. 319-quater).



- **Corruption of a public service officer**, provided for by Art. 320 of the Criminal Code. This crime consists of the acts referred to in Art. 319 of the Criminal Code when they are committed by a public service officer, or the facts referred to in Art. 318 of the Criminal Code when the perpetrator holds the status of public servant.
- **Influence peddling**, provided for by Art. 346-bis. This crime consists in one exploiting or claiming existing or alleged relationships with a Public Official or a Public Service Officer or one of the parties referred to in Art. 322-bis, and thus receiving a gift or promise of money or other benefits from a Private Party for illegally operating as a mediator.
- **Corruption and instigation to corruption of members of bodies of the European Communities and officials of European Communities and of foreign States**, provided for by Article 322-bis of the Criminal Code
- **Penalties for the briber (Art. 321 Criminal Code)**: After mentioning the provisions above, it should be noted that the penalties established in Article 318, paragraph 1, and Article 319, Article 319-bis, Article 319-ter and Article 320 in relation to the cases provided for in Articles 318 and 319, also apply to anyone who gives or promises a public official or a public service officer money or other benefits (with an inevitable broadening of the spectrum of liability of the entity).

#### **B. Computer crimes (Art. 24-bis of the Decree)**

- **Unauthorised access to a computer or telematic system**, provided for by Art. 615-ter of the Criminal Code. This crime consists in a party illegally accessing - i.e., eluding any form, even minimal, of access barriers - a computer or telematic system protected by security measures, or remaining in it there against the will of the person who has the right to exclude the said party accessing.
- **lawful possession and dissemination of access codes to information or telematic systems**, provided for by Art. 615-quater of the Criminal Code. This crime consists in illegally obtaining, holding, producing, reproducing, disseminating, importing, communicating, delivering, making available to others, in any other way, or installing devices, tools, parts of devices or tools, codes, key words or other means suitable for accessing a computer or telematic system protected by security measures, or otherwise providing indications or instructions in this sense, with the aim of obtaining a profit for oneself or others or of causing damage to others.
- **Possession, dissemination, unauthorized installation of computer equipment, devices or programs aimed at damaging or interrupting a computer or telematic system**, provided for in Art. 615-quinquies. This crime consists in illegally obtaining, holding, producing, reproducing, importing, disseminating, communicating, delivering or making available to other, in any other way, or installing equipment, devices or computer software with the aim of illegally damaging a computer or telematic system, the information, data or software contained therein or relevant to it, or otherwise facilitating a total or partial interruption or alteration of its functioning.
- **Illegally wiretapping, prevention or interruption of computer or telematic communications**, provided for in Art. 617-quater. This crime consists in the fraudulent wiretapping of communications relating to a

computer or telematic system or between multiple systems, or preventing or interrupting them. Save where the act constitutes a more serious crime, the same penalty applies to anyone who reveals, in whole or in part, through any means of information to the public, the content of the communications referred to in the first paragraph.

- **Unauthorized possession, distribution and installation of equipment and other means capable of intercepting, preventing or interrupting computer or telematic communications**, provided for by Art. 617-quinquies. This crime consists in conduct of anyone who, outside the cases permitted by law, in order to intercept communications relating to a computer or telematic system or between multiple systems, or to prevent or interrupt them, obtains, holds, produces, reproduces, disseminates, imports, communicates, delivers, or otherwise make available to others, or installs equipment, software, codes, key words or other means capable of intercepting, preventing or interrupting communications relating to a computer or telematic system or between multiple systems.
- **Forgery in computer documents**, provided for by Art. 491-bis of the Criminal Code (this crime extends the criminal prosecution of the crimes provided for in Book II, Title VII, Chapter III of the Criminal Code). This crime consists in the material or ideological forgery of public documents, certificates, authorisations, private deeds or documents, committed by a representative of the Public Administration or a private individual, when the object of forgery is a "public electronic document having evidentiary effects". Electronic document' means the electronic representation of legally relevant acts, facts or data (Law 82/2005, Art.1, para.1, letter p).
- **Damaging information, data and computer software**, provided for by Art. 635-bis of the Criminal Code. This Crime consists in destroying, deteriorating, deleting, altering or suppressing information, data or computer software of other parties, save where this act constitutes a more serious crime.
- **Damaging information, data and computer software used by the State or other public bodies or otherwise of public usefulness**, provided for by Art. 635-ter of the Criminal Code. This crime consists in committing an act aimed at destroying, deteriorating, cancelling, altering or suppressing information, data or computer software used by the State or other public bodies or relevant to them or otherwise of public usefulness, save where the act constitutes a more serious crime.
- **Damaging computer or telematic systems**, provided for by Art. 635-quater of the Criminal Code. This crime consists in destroying, damaging, making in whole or in part unusable the computer or telematic systems of others or seriously hinder their functioning by implementing the conduct referred to in Art. 635-bis or introducing or transmitting data, information or software, save where the act constitutes a more serious crime.
- **Damaging computer or telematic systems of public usefulness**, provided for by Art. 635-quinquies of the Criminal Code. This crime consists in implementing the conduct described in the previous Art. 635-quater, where it is aimed at destroying, damaging, making in whole or in part unusable computer or telematic systems of public usefulness or seriously hindering their functioning.

### **C. Corporate crimes (Art. 25-ter of the Decree)**

- **False social communications** (Art. 2621 of the Civil Code) according to which, outside the cases provided for by Art. 2622, 2622, directors, general managers, executives responsible for drawing up corporate accounting documents, and auditors and liquidators who, in order to obtain an unjust profit for themselves or for others, in the financial statements, reports or other corporate communications the law requires to be addressed shareholders or the general public, present relevant material facts that are not true or omit material facts whose communication is required by law regarding the economic, patrimonial or financial situation of the company or the group to which it belongs, in a manner concretely capable of misleading others, are punished with imprisonment from one to five years.

*The same penalty also applies where false statements or omissions concern assets owned or managed by the company on behalf of third parties.*

For the purposes of 231, a pecuniary sanction of 200 to 400 shares is provided for the entity.

- **Minor crimes** – Pursuant to Art. 2621-bis of the Civil Code, “*ave where the act constitutes a more serious crime, the penalty from six months to three years of imprisonment applies if the acts referred to in Article 2621 are of minor importance, taking into account the nature and size of the company and the methods or effects of the conduct.*

*Save where the act constitutes a more serious crime, the same penalty as in the previous paragraph applies when the acts referred to in Article 2621 concern companies that do not exceed the limits indicated in the second paragraph of Article 1 of the Royal Decree. no. 267 of 16 March 1942<sup>1</sup>. In this case, the crime is prosecutable upon action taken by the company, shareholders, creditors or other recipients of the social communication”.*

For the purposes of Decree no. 231, a pecuniary sanction of 200 to 200 shares is provided for the entity.

Lastly, pursuant to subsequent Article 2621-ter of the Civil Code, “*for the purposes of non-punishability due to the particular triviality of the fact, pursuant to Art. 131-bis of the Criminal Code, the judge evaluates, in a prevalent manner, the extent of any damage caused to the company, to its shareholders or creditors following the acts referred to in Articles 2621 and 2621-bis”.*

- **Control prevented**, provided for by Art. 2625 of the Civil Code. This crime consists in directors preventing or otherwise hindering the performance of control or auditing activities legally attributed to the shareholders to other corporate bodies or auditing firms by concealing documents or putting in place other suitable artifices.
- **Undue return of contributions**, provided for by Art. 2626 of the Civil Code. This crime consists in directors returning or simulating returning contributions to the shareholders or release shareholders from the obligation to pay contributions, outside of cases of legitimate share capital reduction.
- **Illegal distribution of profits and reserves**, provided for by Art. 2627 of the Civil Code. This crime consists in directors distributing profits or advances on profits that were not actually earned or the law requires to allocate to reserves, or distributing legally non-distributable reserves, even when not constituted by profits.

---

<sup>1</sup> This means: “a) in the three financial years preceding the date of filing of the bankruptcy petition or, since the start of the business, if of shorter duration, having had assets of a total annual amount not exceeding €300,000; b) in whatever way it appears, in the three financial years preceding the date of filing of the bankruptcy petition or from the start of the activity if of shorter duration, having achieved gross revenues for a total annual amount not exceeding €200,000; c) having debts, including non-expired debt, not exceeding j€500,000”.

- **Illegal operations on shares or stocks of the company or the controlling company**, provided for by Art. 2628 of the Civil Code. This crime consists in directors purchasing or subscribing shares or stocks outside of the cases permitted by law, thus causing damage to the integrity of the share capital or legally non-distributable reserves; or directors purchasing or subscribing, outside of the cases permitted by law, shares or stocks issued by the controlling company, thus causing damage to the share capital or legally non-distributable reserves.
- **Operations to the detriment of creditors**, provided for by Art. 2629 of the Civil Code. This crime consists in directors carrying out share capital reductions or mergers with other companies or demergers in violation of the laws for creditor protection, and thus cause damage to creditors.
- **Fictitious formation of capital**, provided for by Art. 2632 of the Civil Code. This crime consists in directors and contributing shareholders fictitiously form, even partially, or increase the share capital through the allocation of shares or stocks in an amount that is overall greater than the share capital, reciprocal subscription of shares or stocks, significant overvaluation of contributions in kind or of credits or of the company's assets in the case of transformation.
- **Corruption between private individuals**, rime introduced by Law no. 190 of 6 November 2012 amended by Legislative Decree no. 38 of 15 March 2017. To the purposes of the Decree, this crime exclusively refers to the case described in Art. 2635, para. 3, of the Civil Code, i.e., a top manager or a subordinate offers, promises or gives, even through a third party, money or other undue benefits to directors, general managers, managers responsible for drawing up accounting documents, auditors and/or liquidators of private companies or entities or to anyone who is subject to the direction or supervision of one of them.
- **Unlawful influence on shareholders' meeting**, provided for by Art. 2636 of the Civil Code. This crime consists in determining a majority in the meeting through simulated or fraudulent acts, with the aim of obtaining an unjust profit for oneself or others.
- **Market rigging**, provided for by Art. 2637. This crime consists in spreading false news or carrying out simulated transactions or other artifices concretely capable of causing a significant alteration in the price of non-listed financial instruments or financial instruments for which no request for admission to trading on a regulated market has been submitted.
- **Hindering the exercise of the functions of public supervisory authorities**, provided for by Art. 2638 of the Civil Code. This crime consists in directors, general managers, auditors and liquidators of companies or entities and other parties which are subject by law to public supervisory authorities or are bound by obligations towards them, reporting, in communications the law requires to presented to the said authorities, material facts that are not true, albeit still under verification, regarding the economic, patrimonial or financial situation of parties which are subject to supervision, in order to hinder the exercise of supervisory functions, or them concealing in whole or in part, with other fraudulent means and to the same end, facts that they should have communicated, concerning the said economic, patrimonial or financial situation, even when the information concerns assets owned or managed by the company on behalf of third parties. This crime includes any possible form of knowingly hindering the functions of supervisory authorities by directors, general managers, auditors and liquidators of companies or entities and other parties which are subject by law to public supervisory authorities or are bound by obligations towards them, including the non-presentation of the legally required communications.

**D. Crimes against the person (Art. 25-septies of the Decree)**

- ***Involuntary manslaughter***, provided for by Art. 589 of the Criminal Code. This crime consists in causing the death of a person through negligence, in violation of the rules on the prevention of accidents at work.
- ***Serious or very serious negligent injury***, provided for by Art. 590 of the Criminal Code. This crime consists in negligently causing serious or very serious personal injury to others, in violation of the rules on the prevention of accidents at work.

**E. Receiving, laundering and use of money, assets or benefits of illicit origin and self-laundering (Art. 25-octies of the Decree)**

- ***Receiving***, provided for by Art. 648 of the Criminal Code. This crime consists in purchasing, receiving or concealing, outside of cases of participation in a crime, money or things deriving from a crime of any type, or helping having them purchased, received or concealed, in order to obtain profit for oneself or others.
- ***Laundering***, provided for by Art. 648-bis of the Criminal Code. This crime consists in substituting or transferring, outside of cases of participation in a crime, money, assets or other benefits deriving from criminal activity, or carry out other operations in relation to them, in such a way as to hinder the identification of their criminal origin.
- ***Use of money, assets or benefits of illicit origin***, provided for by Art. 648-ter of the Criminal Code. This crime consists in using, outside of cases of participation in a crime and the cases provided for by Articles 648 and 648-bis, money, assets or other benefits deriving from crime in economic or financial activities.
- ***Self-laundering***, provided for by Art. 648-ter.1 of the Criminal Code. This crime consists in the conduct of anyone who, after having committed or participated in a crime, uses, substitutes or transfers in economic, financial, entrepreneurial or speculative activities, the money, assets or other benefits deriving from the said crime, in such a way as to concretely hinder the identification of criminal origin of the said money, assets or benefits. A specific mitigating circumstance is provided for when the money, assets or other benefits derive from the commission of a crime punishable by a maximum term of imprisonment of less than five years. In any case, the penalties provided for the basic crime apply when the money, assets or other benefits derive from a crime committed under the conditions or with the aims of mafia-type associations (Art. 416-bis of the Criminal Code). Outside of the cases listed above, conduct whereby money, assets or other benefits are used for mere personal use or enjoyment is not punishable.

**F. Crimes relating to non-cash payment instruments and fraudulent transfer of assets (Art. 25-octies.1)**

- ***Unauthorised use and forgery of payment instruments other than cash***: provided for by Art. 493-ter of the Criminal Code. This crime consists in anyone unduly using, without being their holder, credit or payment cards or

any other similar document that allows to withdraw cash or purchase of goods or services, or any other payment instrument other than cash, in order to gain profit for oneself or others.

- **Possession and distribution of equipment, devices or computer software aimed at committing crimes involving payment instruments other than cash:** provided for by Art. 493-quater. Save where the act constitutes a more serious crime, this crime consists in producing, importing, exporting, selling, transporting, distributing, making available or otherwise obtaining for oneself or others, equipment, devices or computer software which, due to their technical and construction or design characteristics, were primarily realised or specifically adapted to commit crimes involving payment instruments other than cash, when the producing, importing, exporting, selling, transporting, distributing, making available or otherwise obtaining these equipment, devices or computer software is aimed at directly using them or permitting other to use them to commit the afore-mentioned crimes.
- **Computer fraud:** provided for by Art. 640-ter of the Criminal Code. This crime consists in, altering in any way the functioning of a computer or telematic system or computer or telematic system software contained in or related to a computer or telematic system, in order to obtain, for oneself or others, an unjust profit to the detriment of others.
- **Fraudulent transfer of property:** provided for in Art. 512-bis of the Criminal Code. This crime consists in fictitiously attributing to others the ownership or availability of money, assets or other benefits, in order to evade the legal provisions on patrimonial or smuggling prevention, or facilitating the commission of one of the crimes referred to in Articles 648, 648-bis and 648-ter of the Criminal Code.

#### **G. Copyright infringement crimes (25- nonies)**

- Based on the scenario that emerged following the risk self-assessment carried out within S.C.F., Art. 171-Bis of Law no. 633 of 22 April 1941 appears significant, as it punishes anyone who unlawfully duplicates, for profit, computer software or imports, distributes, sells, holds for commercial or entrepreneurial purposes or leases software contained in media not marked by SIAE (the Italian Society of Authors and Publishers). These acts are also punished when they involve any means intended solely to allow or facilitate the arbitrary removal or functional evasion of devices applied to protect a computer software.
- The said Law also punishes anyone who, in order to make a profit, reproduces, transfers to another medium, distributes, communicates, presents or demonstrates in public the contents of a database in violation of the provisions of Articles 64-quinquies and 64 sexies, or extracts or re-uses a database in violation of the provisions of Articles 102-bis and 102-ter of the same law, or distributes, sells or leases a database.
- The Decree also covers the following:
  1. Art. 171, para. 1, letter a-bis) which punishes anyone who makes available a protected intellectual work or part of it to the public, by entering it into a telematic network system, through connections of any kind.
  2. Art. 171, para. 3, which provides for an increase in the penalty to be applied for the crime referred to in the previous point when the perpetrator commits it on a work of which he/she is not the author and which is not intended for

*publication, by usurping authorship of the work, or distorting, mutilating or making any other change to the work, and thus harms the author's honour or reputation.*

3. *Art. 171-ter, which punishes anyone who, for profit and for non-personal use:*

- *Unlawfully duplicates, reproduces, broadcasts or publicly disseminates, in whole or in part, any intellectual work intended for television, cinema, sales or rental, discs, tapes or similar media or any other media containing phonograms or videograms of musical, cinematographic or similar audiovisual works or sequences of moving images;*
- *illegally reproduces, broadcasts or disseminates in public, by any means, works or parts of literary, theatrical, scientific or didactic, musical or theatrical-musical or multimedia works, even when these works are part of collective or composite works or databases;*
- *although not having participated in the duplication or reproduction, introduces into the territory of the State, holds for sale or distribution, distributes, puts on the market, rents out or otherwise transfers in any capacity, projects in public, broadcasts by television, with any procedure, or by radio, makes public listening of the illegal duplications or reproductions referred to in the two previous points;*
- *holds for sale or distribution, places on the market, sells, rents, assigns in any capacity, projects in public, broadcasts by radio or television, with any method, video cassettes, music cassettes, any medium containing phonograms or videograms of musical, cinematographic or audiovisual works or sequences of moving images, or other medium not bearing the SLAE mark required by copyright law or bearing an altered SLAE mark;*
- *in the absence of an agreement with the legitimate distributor, broadcasts or disseminates by any means an encrypted service received by means of equipment or parts of equipment capable of decoding conditional access transmissions;*
- *introduces into the territory of the State, holds for sale or distribution, distributes, sells, rents, assigns in any capacity, commercially promotes, installs special decoding devices or elements that allow access to an encrypted service without paying the relevant fee;*
- *manufactures, imports, distributes, sells, rents, assigns in any capacity, advertises for sale or rental, or holds for commercial purposes, equipment, products or components, or provides services which have as their prevalent aim or commercial use the circumvention of effective technological measures, or are primarily designed, produced, adapted or created with the purpose of enabling or facilitating the circumvention of the said measures;*
- *abusively removes or alters the electronic information referred to in Article 102-quinquies<sup>2</sup>, or distributes, imports for distribution, broadcasts by radio or television, communicates or makes available to the public works or other protected materials from which electronic information has been removed or altered.*

*More severe penalties are provided for anyone who:*

- *reproduces, duplicates, broadcasts or distributes abusively, sells or otherwise places on the market, assigns for any reason or abusively imports more than fifty copies or specimens of works protected by copyright and related rights;*
- *in violation of Article 16, for profit purposes, communicates a work of mind protected by copyright, or part of it,*

---

<sup>2</sup> Pursuant to Art. 102-quinquies, "electronic information on the rights regime identifies the work or protected material, its author or any other holder of rights. This information may also contain indications regarding the terms or conditions of use of the work or materials, as well as any number or code representing the information itself or other identifying elements".

*to the public, by placing it in a telematic network system through concessions of any kind;;*

- *commits the acts set out in paragraph 1 by carrying out, in an entrepreneurial manner, the activities of reproduction, distribution, sale or marketing, import of works protected by copyright and related rights;*
- *promotes or organises the illegal activities referred to in paragraph 1.*

*Conviction for one or more of the above-described crimes entails, inter alia, the suspension for a period of one year of the concession or authorisation for radio and television broadcasting for the exercise of the productive or commercial activity.*

4. *Art. 171-septies, which punishes producers or importers of media not subject to the marking referred to in Article 181-bis, who do not communicate SIAE the data necessary for the unequivocal identification of the said media within thirty days from the date of placing the said media on the market in the Italian territory. This provision also punishes anyone who falsely declares to have fulfilled the obligations referred to in Article 181-bis, paragraph 2, of this Law (obligations deriving from the legislation on copyright and related rights).*
5. *Art. 171-octies which punishes anyone who, for fraudulent purposes, produces, offers for sale, imports, promotes, installs, modifies, uses for public and private purposes equipment or parts of equipment suitable for decoding conditional access audiovisual broadcasting over the air, via satellite, via cable, in both analogue and digital form<sup>3</sup>.*

#### **H. Inducement not to make statements or to make false statements to a judicial authority (Art. 25-decies)**

- ***Inducing not to make statements or to make false statements to the judicial authority***, *this crime is punished under Art. 377-Bis of the Criminal Code, according to which, where the act constitutes a more serious crime, anyone who, by means of violence or threats, or by offering or promising money or other benefits, induces a person called upon to make statements before a Judicial Authority that can be used in criminal proceedings, not to make statements or to make false statements, when this person has the right to silence.*

#### **H. Employment of third-country nationals whose stay is irregular (Art. 25-duodecies)**

- ***Employment of third-country nationals whose stay is irregular***. *This crime is regulated by Art. 22 paragraph 12-bis of Legislative Decree no. 286 of July 25, 1998, n. 286, and consists in an employer employing foreign workers that are deprived of the residence permit provided for by this article, or whose permit has expired and for which renewal has not been requested within the terms, or has been revoked or cancelled.*
  - a) *when employed workers are more than three;*
  - b) *when the employed workers are minors of non-working age;*
  - c) *when the employed workers are subjected to other particularly exploitative working conditions referred to in Art. 603-Bis, para. 3, of the Criminal Code,*
    - *more severe penalties are provided for to punish the conduct of promoting, directing, organising, financing or*

---

<sup>3</sup> All audiovisual signals transmitted by Italian or foreign broadcasters in such a way as to make them visible exclusively to closed groups of users selected by the entity that broadcasts the signal, regardless of the imposition of a fee for the use of this service, are considered to be conditional access.



*transporting foreigners into the territory of the State or other acts aimed at making foreigners illegally enter Italy or another State of which they are not citizens or in which have to right to reside, when:*

- a) the act concerns the illegal entry or presence in the territory of the State of five or more persons;*
- b) the transported persons were exposed to life or safety danger in order to have them illegally enter or stay in Italy;*
- c) the transported persons were subjected to inhuman or degrading treatment in order to secure their illegal entry or stay;*
- d) the act is committed by three or more persons in collusion with each other or using international transport services or forged or altered documents or documents obtained illegally;*
- e) the perpetrators of the crime have access to weapons or explosive materials.*
- *When two or more of the cases under letters a), b), c), d) and e) above occur, the penalty provided for therein is increased.*
- *The penalty is increased when the acts:*
  - a) are committed with the aim of recruiting people for prostitution or sexual or labour exploitation or involve the entry of minors to be employed in illegal activities, in order to facilitate their exploitation;*
  - b) are committed for obtaining profit, even indirectly*
- *Furthermore, encouraging the stay of foreigners in the territory of the State in order to gain an unfair profit from their illegal status or in the framework of other activities contrary to illegal immigration, as per Art. 12 of Legislative Decree no. 286 of 25 July 1998, n. 286, is punished.*

#### **I. Racism and xenophobia (25-terdecies)**

***Racism and xenophobia***, originally regulated by Art. 3 paragraph 3 bis of Law no. 654 of 3 October 1975, n. 654 and currently by Art. 604-bis paragraph 3 of the Criminal Code. The commission is punished of propaganda crimes or solicitation or incitement to commit crimes based on racial, ethnic and religious discrimination, when they are committed in such a way as to create a concrete risk of diffusion, are based in whole or in part on the denial, serious minimisation or apology of the Holocaust or of crimes of genocide, crimes against humanity and war crimes, as defined by the Articles 6, 7 and 8 of the Statute of the International Criminal Court. ~~Furthermore, participation in or assistance to the activities of organizations, associations, movements or groups whose aims include inciting discrimination or violence for racial, ethnic, national or religious reasons is prohibited~~

#### **L) Tax crimes (Art.25-quinquiesdecies)**

- ***Tax crimes***, regulated by Legislative Decree no. 74 of 10 March 2000 and supplemented by Legislative Decree no. 75 of 14 July 2020 bearing “Implementation of EU Directive 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law” (PIF Directive). The following crimes are punished:
  - *fraudulent tax returns made by using invoices or other documents for non-existent transactions*
  - *fraudulent tax returns made by other means*

- *issuing invoices or other documents for non-existent transactions*
  - *concealment or destruction of accounting documents*
  - *fraudulent evasion of tax payment*
  - *failure to declare, incorrect declaration, undue compensation, when even partly committed in another European member state for evading VAT*
- ***Fraudulent tax returns by using invoices or other documents for non-existent transactions (Art. 2, paragraph 1 and paragraph 2-bis, Legislative Decree 74/2000):*** *This crime consists in reporting, in a tax return, fictitious liabilities based on invoices or other documents for non-existent transactions, in order to evade income or value added taxes.*

*The act is considered to have been committed by using invoices or other documents for non-existent transactions when such invoices or documents have been recorded in the mandatory accounting records, or are held for evidence against the financial administration.*

*“invoices or other documents for non-existent transactions” means invoices or other documents with similar evidentiary effects under tax law which are issued, in whole or in part, for transactions that had been not actually carried out, or which indicate consideration or value added tax in a higher amount than the actual amount, or which refer a transaction to parties other than the actual parties.*

*For the crime, relevant ‘other documents’ are all those which attest to the provision of a service and therefore the validity of a tax deduction or credit, such as invoices, tax receipts, customs documents, credit notes, fuel logs.*

- ***Fraudulent tax return through other artifices (Art. 3 of Legislative Decree 74/2000):*** *The crime is committed when, outside the cases provided for in Article 2 above, in order to evade income tax or value added tax, the perpetrator of the crime, by (i) carrying out objectively or subjectively simulated transactions or (ii) using false documents or other fraudulent means capable of hindering verification by and misleading tax authorities, in income tax or VAT returns declares an amount of assets lower than the actual amount or fictitious liabilities or receivables and withholdings, when, jointly:*

*a) the evaded tax is higher, for each individual tax, than €30,000;*

*b) the total of assets subtracted from taxation, even through the indication of fictitious liabilities, (i) is greater than five percent of the total assets indicated in the tax return, or in any case, (ii) is greater than €1,500,000, or (iii) if the total of fictitious receivables and withholdings that reduce the tax is greater than five percent of the amount of the tax or €30,000.*

*The act is considered to have been committed by using false documents for non-existent transactions when such documents have been recorded in the mandatory accounting records, or are held for evidence against the financial administration.*

*The mere violation of the obligations of invoicing and recording assets in accounting records or the mere indication in the invoices or recordings of assets lower than the current assets do not constitute fraudulent means.*

- **Issuing invoices or other documents for non-existent transactions (Art. 8 of Legislative Decree 74/2000):** This crime consists in issuing invoices or other documents for non-existent transactions in order to allow third parties to evade income tax or value added tax.

*The issuing of multiple invoices or documents for non-existent transactions during the same tax period is considered as a single crime.*

- **Concealment or destruction of accounting documents (Art. 10 of Legislative Decree 74/2000):** This crime occurs when a person, (i) in order to evade income or value added taxes, or (ii) to allow third parties to do so, conceals or destroys, in whole or in part, accounting records or documents which must be kept, in such a way as to prevent the reconstruction of income or turnover.

*The material object of the criminal conduct consists of the accounting and documentary records which must be kept according to tax or civil law which distinguish between absolutely mandatory books (journal, stock book, etc.) and relatively mandatory records such as those required by the size of the company.*

*These documents have a fundamental instrumental function in protecting creditors, including tax authorities, as their preservation allows or in any case facilitates the detection and understanding of business transactions and business income as well as the discovery of traces of any tax crime.*

*Concealment consists in physically hiding the documents (refusal to deliver them or keeping them in a place other than that indicated to the tax authorities is generally not relevant). Destruction hand, consists in the physical elimination or in making entries illegible or unusable in whole or in Art.*

- **Fraudulent evasion of tax payment (Art. 11 of Legislative Decree 74/2000):** This crime occurs::  
a) when a person - in order to avoid paying income tax or value added tax or interest or administrative penalties relating to the said taxes for a total amount exceeding €50,000 - simulates sales or carries out other fraudulent acts on his/ her own or other people's assets capable of rendering the compulsory collection procedure, in whole or in part, ineffective;  
b) when a person - in order to obtain for him/ herself or others a partial payment of tax and related accessories - declares in the documentation submitted for the purposes of the tax transaction procedure (i) assets for an amount lower than the actual amount or (ii) fictitious liabilities a total greater than €50,000. f the amount referred to in the previous paragraph is greater than €200,000, imprisonment from one year to six years shall apply.

*Simulated transfer occurs in cases where the intention to transfer ownership of an asset, manifested externally, does not correspond to the real intention of the parties, while 'other fraudulent acts' are all acts other than simulated conveyance carried out in order to render collection ineffective. Consider the creation of real rights of enjoyment on real estate, business rental contracts, the recognition of non-existent liabilities in order to remove assets from the enforcement procedure.*

*The tax transaction procedure is the transactive procedure between the authorities and a taxpayer. It aims to avoid irreversible bankruptcy of the entrepreneur through the reduction or deferral of tax and contributory debts provided for by the new Business Crisis Code in Articles 63 and 88 of Legislative Decree no. 14/2019.*

- **Untruthful tax return (Art. 4 of Legislative Decree 74/2000), Omitted tax return (Art. 5. of Legislative Decree no. 74/2000), Undue compensation (Art. 10-quater of Legislative Decree**

**74/2000):** Legislative Decree no. 75 of 14 July 2020 implemented Directive (UE) 2017/1371 (PIF Directive) “on the fight against fraud to the Union's financial interests by means of criminal law” which has extended the liability referred to in the Decree also to the crimes of untruthful tax return, omitted tax return and undue compensation, **if committed, even partially, in the territory of another EU member state for evading value added tax for a total amount of not less than €10,000,000.**

*Untruthful tax return consists in presenting an income tax return or a value added tax return in which assets are declared of an amount lower than current assets or non-existent liabilities, in order to evade the said taxes.*

*For the crime to exist, two conditions must be met at the same time, as follows: the evaded tax must be greater than €100,000 and the overall assets removed from taxation, even through the declaration of non-existent liabilities, must be greater than ten percent of the overall assets declared in the tax return or is greater than €2,000,000.*

*Omitted presentation of a tax return is punished with imprisonment from two to five years. The crime consists in failure to present mandatory income tax return or value added tax return, with the aim of evading one of the said taxes, when the evaded tax is higher, with reference to one tax only, than 50,000. A tax return submitted within ninety days of the deadline, not signed not drawn up on a form conforming to the prescribed template is not considered to have been omitted. Undue compensation consists in failing to pay due amounts by compensating them pursuant to Art. 17 of Legislative Decree no. 241 of 1997 but with non-due or non-existent credit. Therefore, a failure to pay is not sufficient to constitute the crime, as failure to pay must be formally ‘justified’ upstream by a compensation between the amounts owed to the tax authorities and the credits towards the taxpayer, which in reality are not due or do not exist. This is because the conduct of compensation is necessary to express the deceptive or fraudulent component inherent in the crime and is the factor this crime from simple failure to pay.*

In the following Special Part, this document describes the Company's activities that are considered sensitive due to the inherent risk of committing crimes, such as those listed herein, providing, for each of the sensitive activities, prevention principles and protocols.

The Company undertakes to constantly evaluate the relevance of any further crimes, current and future, with a view to constantly and systematically updating this Model.

## **8. Recipients of the Model**

The Model applies to:

- a) Whoever is vested with a management, administration, direction or control function in the Company or in one of its autonomous organisational units, even *de facto*;
- b) The Company's employees, even if seconded abroad to carry out their activities;

- c) All those individuals who collaborate with the Company under a para-subordinate employment relationship, such as project collaborators, temporary workers, agency workers, etc.;
- d) Whoever works according to a mandate or on behalf of the Company although not belonging to it, such as lawyers, promoters, agents or consultants;
- e) Whoever acts in the interest of the Company insofar as linked to it by contractual legal relationships or other agreements, eg joint-venture partners or partners for the implementation or acquisition of a business project.

Any doubts regarding the applicability or the methods of application of the Model to a third party or class of third parties are resolved by the Supervisory Body. In general terms, and without prejudice to the specific provisions contained in the relevant regulation, the Supervisory Body a) identifies the types of legal relationships with any parties external to the Company, to whom it is appropriate to apply the provisions contained in the Model due to the nature of the activity carried out; b) establishes the communication methods used for the procedures the external parties involved need to observe for compliance with the Model.

All said recipients are required to promptly comply with the provisions contained in the Model and its implementation procedures.

## **9. Supervisory Body**

### **9.1. Function**

In compliance with the Decree, the Company establishes an autonomous, independent and competent Supervisory Body in matters of risk control connected to the specific activity carried out by the Company and its legal profiles.

The Supervisory Body has the task of constantly monitoring the following:

- compliance with the Model by the consortium bodies, employees and consultants of the Company;
- the Model's actual effectiveness in preventing crimes referred to in the Decree from being committed;
- implementation of the provisions contained in the Model while performing the Company's activities;

- Model updating whenever it needs modifying due to changes occurred in the company structure and organisation or in the relevant regulatory framework.

The Supervisory Body shall adopt its own Operating Regulations, approve their contents and present them to the Board of Directors for approval at the first available meeting following the Body's appointment.

## **9.2. Appointment of the members of the Supervisory Body**

In compliance with the following parameters, the Company has opted for **a single-member Supervisory Body**: the designated person is appointed by the Board of Directors via a reasoned provision, which also establishes the annual remuneration to be paid, as well as the budget annual amount to be allocated to the performance of the activities for which the Supervisory Body is responsible.

The choice of the person must be based exclusively on the following requirements:

- autonomy, understood as the ability to decide autonomously and with full exercise of technical discretion in carrying out one's functions;
- independence, understood as the condition of absence of ties, interests or forms of interference with other company functions or third parties, such as to jeopardise the objectivity of decisions and actions;
- professionalism, understood as a set of specialised technical tools and knowledge (legal, accounting, statistical, business and organisational), such as to allow the assigned activity to be carried out effectively;
- continuity of action, understood as the ability to operate with an adequate level of commitment, mainly aimed at monitoring the Model.

After the appointed person has formally accepted the office, the decision is notified to all company levels via internal communication.

The Supervisory Body may take advantage of an expert in workplace safety.

The Supervisory Body remains in office for 3 (three) years, starting from the day of acceptance of the appointment, and can be re-elected.

### **9.3. Eligibility Requirements. Forfeiture and replacement.**

The person appointed as single member of the Supervisory Body shall be professional, honourable and independent, have functional autonomy and continuity of action and be provided with the competence necessary to carry out the tasks assigned according to the Decree.

The appointed person shall not be in any of the following ineligibility and/or incompatibility conditions:

- conviction (even with a non-final sentence) for committing one of the crimes provided for by the Legislative Decree No 231/01;
- interdiction, incapacitation, bankrupt or sentence (even in the first instance) to a penalty involving interdiction, even temporary, from public office or the incapacity to perform managerial offices.

The occurrence of even one of the above conditions entails ineligibility as member of the Supervisory Body and, if elected, automatic forfeiture, without the need for resolution of dismissal by the Board of Directors; the latter shall provide for his/her replacement within 45 (forty-five) days of becoming aware of the cause of ineligibility/incompatibility, or in any case at the first available meeting.

Furthermore, the appointed person shall not:

- hold other operational offices within the Company;
- be in a clear or potential situation of conflict of interest with respect to the purposes pursued by the Company.

### **9.4. Dismissal and withdrawal**

The member of the Supervisory Body may only be dismissed via a resolution by the Board of Directors and only in the event of just cause.

The following conditions legitimise dismissal for just cause:

1. failure to fulfil the obligations inherent in the assigned task;
2. lack of good faith and diligence in the performance of one's duties;
3. subsequent inability to act.

In the event of just cause, the Board of Directors removes the appointed person from his/her office as member of the Supervisory Body and, after adequate motivation, reorganises the Supervisory Body within 45 (forty-five) days of knowledge of the just cause for dismissal, or in any case at the first available meeting.

In the meantime, the office is performed by the oldest member of the Board of Auditors.

The person representing the Supervisory Body can withdraw at any time from the office, subject to a minimum notice of 45 (forty-five) days, with written and motivated communication to the Board of Directors.

In the event of withdrawal, the Board of Directors shall reorganise the Supervisory Body within 45 (forty-five) days of the written communication referred to above, or at the first available meeting thereafter.

## **9.5. Powers**

In order to carry out its assigned tasks, the Supervisory Body is vested with all powers of initiative and control over all company activities and personnel levels. Furthermore, it hierarchically and exclusively depends on the Board of Directors.

The Supervisory Body's duties and responsibilities cannot be audited by any other corporate body or structure, without prejudice to the fact that the Board of Directors has the power to verify the coherence between the former's activities and the internal corporate policies.

The Supervisory Body carries out its functions in coordination with other bodies or control functions existing within the Company, or which in any case carry out the aforementioned control activity in the name and on behalf of the Company.

In particular, the Supervisory Body:

- coordinates with the HR manager for all matters concerning staff training in matters related to Legislative Decree No 231/2001;
- constantly monitors the regulatory framework concerning the Decree to update the Model, if necessary, after obligatorily consulting with the Chairman of the Board of Directors;



- develops the contractual clauses that regulate the application of the Model to persons external to the Company;
- coordinates with the company functions that carry out activities at risk for all aspects relating to the implementation of the operational procedures for implementing the Model.

In monitoring the effective implementation of the Model, the Supervisory Body is vested with powers and duties which it exercises in compliance with the law and the individual rights of workers and interested parties, structured as follows:

- a) carrying out or arranging for the carrying out of periodic inspections under his/her direct supervision and responsibility;
- b) accessing all information regarding the Company's sensitive activities;
- c) requesting information or the production of documents regarding sensitive activities from all employees of the Company and, where necessary, from the Directors, the Board of Auditors and the persons in charge, in compliance with the provisions of the legislation on accident prevention, safety and health protection in the workplace;
- d) requesting information or the production of documents regarding sensitive activities from collaborators, consultants, agents and external representatives of the Company, and in general from all persons to whom the Model is addressed, identified as provided for in Section 8;
- e) taking advantage of help and support by the employees;
- f) using external consultants if problems arise that require the assistance of specific skills;
- g) proposing to the body or function holding disciplinary power the adoption of the necessary sanctions, as per the following Section 11;
- h) periodically checking the Model and, where necessary, proposing any changes and updates to the Board of Directors;
- i) defining, in agreement with the HR manager, the staff training programmes in the context of '231' issues;
- j) drafting on a periodical basis (at least once a year) a written report to the Board of Directors, with the minimum contents established in the following section.

- k) In the case of serious and urgent events occurring during the performance of one's activities, the Board of Directors shall be informed immediately;
- l) identifying and periodically updating (after consulting the HR manager and the manager of the area the contract/relationship refers to) the types of legal relationships with parties external to the Company to which it is appropriate to apply the Model, as well as determining the methods of communicating the Model to such parties and the procedures necessary for compliance with the provisions contained therein.

At the end of each year of office, the Supervisory Body determines its own budget for the following year, submitting it to the attention of the Board of Directors for approval at the first available meeting thereafter.

#### **9.6. Information flows to and from the Supervisory Body**

The Supervisory Body shall report only to the Board of Directors, including on relevant facts of its office or on any urgent critical issues of the Model that may emerge during its supervisory activity.

The Supervisory Body shall submit, at least annually, a written report containing the following specific information:

- summary of the activities and controls carried out throughout the year;
- any discrepancies between the operating procedures implementing the provisions contained in the Model and the provisions themselves;
- possible new areas in which the crimes already provided for by the Decree may be committed;
- check of reports received from external or internal parties regarding potential infringements of the Model;
- results of the checks regarding the above reports;
- any disciplinary proceedings and any sanctions applied to the Company, with exclusive reference to those inherent to risky activities;
- general assessment of the effective functioning of the Model, with any proposals for additions and improvements as to form and content;

- any changes to the regulatory framework;
- statement of expenses incurred.

By defining an operating procedure, the Supervisory Body can establish the other types of information that the persons in charge of managing sensitive activities are required to transmit, as well as the frequency and methods with which such communications is to be forwarded to said Body.

All company personnel and external persons to whom this document is addressed have the right to communicate directly with the Supervisory Body to report any infringements of the Model.

Pursuant to art. 6, paragraph 2-bis, of Legislative Decree No 231/2001, SCF has established its own internal channel for managing reports of infringements, as required by Legislative Decree No 24/2023<sup>4</sup> (known as '**whistleblowing reports**'), and has adopted the internal procedure on whistleblowing (*organisational procedure No 12 relating to the reporting of illicit acts, known as 'whistleblowing'*), which identifies the Company's Supervisory Body as the reports' manager.

As defined in the Policy (*Subject matter of the whistleblowing*), among the behaviours, acts or omissions harming the public interest or the integrity of the organisation itself, *conducts that are relevant pursuant to Legislative Decree No 231/2001 and infringements of the Organisation, Management and Control Model adopted pursuant to Legislative Decree No 231/2001 are subject to reporting.*

In his/her quality as Whistleblowing Manager, the Supervisory Body provides its support to carry out the most appropriate checks to ascertain the truthfulness and validity of the facts reported and, if necessary, to acquire information from the Whistleblower and the alleged person responsible for the reported infringement.

If, following the investigations, the Whistleblowing Manager concludes that the reported facts are well-founded and that the infringement can be attributed to one or more persons, the Supervisory Body provides its support to suggest any corrective actions on the Model.

If, following the investigations, the Whistleblowing Manager does not reach the aforementioned conclusions, the Supervisory Body may always propose any corrective measures or additions to the Model that it deems appropriate to reduce the risk of commission of crimes or

---

<sup>4</sup> Legislative Decree No 24/2023 (arts. 4 and 5)

infringements similar to those reported. If necessary, the Supervisory Body may make recommendations to persons involved in the reported incident.

Any person involved in managing whistleblowing acts in such a way as to protect the Whistleblowers against any type of retaliation, discrimination or penalisation, especially by ensuring compliance with all the provisions of the implementing decree of Directive (EU) No 2019/1937, as referred to in art. 2 paragraph 2-bis of Legislative Decree No 231/2001. Furthermore, the Whistleblower's identity shall be kept confidential, without prejudice to legal obligations.

In any case, any person involved in managing whistleblowing is required to maintain the strictest confidentiality of any and all information that he/she may become aware of in performing his/her functions, both towards internal and external parties to the Company.

The guarantees and protection measures in favour of the Whistleblower as provided for in the Policy are referred to by the Model as an integral part of this document.

In addition to the reports relating to general infringements described above, the Supervisory Body shall receive all information relating to disciplinary proceedings initiated as to reports of infringements of the Model and sanctions imposed (including measures taken against employees) or to the archiving of said proceedings with appropriate reasons.

#### **10. Provision of goods or services by consortia and/or other companies**

The provision of goods or services by consortia and/or other companies, with particular reference to goods and services that may concern sensitive activities, shall be regulated in the form of a written contract. Said contract shall be notified to the Company's Supervisory Body.

The contract between the parties must include the following clauses:

- obligation on the part of the entity providing the goods/services to certify the truthfulness and completeness of the documentation produced and the information given to the Company;
- commitment by the entity providing the goods/services to comply, during the duration of the contract, with the provisions set out in the Code of Ethics and the Model;

- obligation to comply with any requests for information, data or news from the Company's Supervisory Body, provided that such obligation is expressly provided for in the contracts or mandates that bind the persons external to the Company.

Failure to comply with one of the above conditions shall be duly motivated and communicated in writing to the Supervisory Body of each of the parties involved.

## **11. Communication and training**

The communication relating to the Model is entrusted to the staff manager, which guarantees its dissemination and effective knowledge to all the recipients referred to in Section 8 through the means they deem most appropriate.

The Supervisory Body determines the methods to communicate with the recipients of the Model external to the Company.

With the key assistance of the Supervisory Body, the Company is required to implement and formalise specific training plans. The aim is to ensure effective knowledge of the Decree, the Code of Ethics and the Model by all company departments and functions.

For the implementation of the Model, staff training is managed by the staff manager in close cooperation with the Supervisory Body, which ensures that training programmes are delivered promptly.

The Company provides for means and methods that always ensure the traceability of training initiatives and the formalisation of participants' attendance, as well as the possibility of evaluating their level of learning and course enjoyment, with the aim to develop new training initiatives and improve those currently underway, also through comments and suggestions on content, material, teachers, etc.

The training is carried out by experts in the discipline dictated by the Decree and can also be carried out remotely or through the use of IT systems; its contents are assessed by the Supervisory Body.

## **Special Part**

## 1. Introduction

Pursuant to the provisions of art. 6 letter a) of the Decree, via a process of risk mapping, evaluation of the activities, existing controls and the corporate context in which it operates (known as 'control and risk self-assessment') the Company has identified the sensitive activities (divided by crime type and listed in the following sections), within which crimes among those provided for by the Decree may potentially be committed.

In order to prevent or mitigate the risk of committing such crimes, the Company has therefore formulated general principles of conduct and general prevention protocols applicable to all sensitive activities, as well as specific prevention protocols for each of the risky activities thus identified.

## 2. General principles of conduct

All recipients of the Model, as identified in Section 8 of the General Part, adopt rules of conduct compliant with the law, the provisions contained in this document and the principles contained in the Code of Ethics, in order to prevent the occurrence of the crimes envisaged by the Decree.

In particular, the principles of conduct identified in the Code of Ethics, hereinafter referred to in full and referring to the various types of recipients and/or counterparties, constitute a prerequisite and an integral part of the control protocols referred to in the following Section 3.

For the purposes of adopting and implementing the Organisation, Management and Control Model, the Company also undertakes to implement the specific protocols indicated below.

## 3. General prevention protocols

In the context of all operations concerning sensitive activities referred to in the following sections, the general prevention protocols implement the following principles:

- the Company's decision-making process and decision implementation respond to the principles and provisions contained in the provisions of law, in the articles of association and in the Code of Ethics;

- the management, coordination and control responsibilities within the Company are adequately formalised;
- the levels of hierarchical dependence are formalised and the various tasks within the Company are described;
- the formation phases and authorisation levels of the Company's acts are always documented in writing and can always be recreated;
- the system of mandates and external signature powers are consistent with the responsibilities assigned to each director and knowledge of such powers by external parties is guaranteed by adequate communication and advertising tools;
- the assignment and exercise of powers within a decision-making process are consistent with positions of responsibility and with the relevance and/or criticality of the underlying economic transactions;
- there is no subjective identity between those who make or implement decisions, those who must provide accounting evidence of them and those who are required to carry out the checks as per the law and the procedures contemplated by the internal control system;
- For all risky operations concerning sensitive activities, adequate prevention procedures are implemented and carried out and an internal manager is identified for the implementation of the operation. Unless otherwise stated, said internal manager corresponds to the General Manager (hereinafter '**Internal Manager**').

The Internal Manager:

- √ can request information and clarifications from all company functions, operating units or individuals who are or have been involved in the risky operation;
- √ promptly informs the Supervisory Body of any critical issues or conflicts of interest;
- √ may consult the Supervisory Body in all cases of ineffectiveness, inadequacy or difficulty in implementing the prevention protocols or the operational procedures for their implementation, as well as in order to obtain clarifications regarding the objectives and methods of prevention envisaged by the Model;
- access to Company data complies with Legislative Decree No 196 of 2003 and subsequent amendments or additions, including regulatory ones;



- documents relating to decision-making and decision implementation are archived and stored by the competent function; access to documents already archived is permitted only to persons authorised according to the Company's operating procedures, as well as to the Board of Statutory Auditors and to the Supervisory Body;
- the choice to use external consultants shall be motivated and occur on the basis of requirements of professionalism, independence and competence;
- the systems of rewarding remuneration allocated to employees and collaborators respond to realistic objectives which are consistent both with the tasks and activities performed and with the responsibilities assigned;
- The Company's financial flows, both incoming and outgoing, are constantly monitored and always traceable;
- all forms of donation aimed at promoting goods, services or the image of the Company must be authorised, justified and documented;
- the Supervisory Body verifies that the company operating procedures (which regulate the activities at risk and constitute an integral part of the Model) fully implement the principles and provisions contained in this Special Part, and that they are constantly updated, also on the proposal of the Body, in order for the purposes of this document to be achieved;
- in the event of modification of existing procedures or if they are found to be inadequate with respect to this Model and/or the real dynamics of the Company's commercial, economic and financial activity, the Internal Manager consults with the Supervisory Body, which forwards suitable proposals to integrate the existing procedures. In case of disagreement regarding the strategic choices to be adopted, the will of the Internal Manager prevails.

## **A. Crimes against Public Administration**

For the purposes of the Decree, 'Public Administration' involves all those subjects, whether public or private, who perform a public function or a public service.

The term '**public function**' is related to the activities governed by public law provisions that pertain to legislative functions (State, Regions, Provinces with special statutes, etc.), administrative functions (members of state and territorial administrations, Law Enforcement, members of supranational administrations, members of the Authorities, members of the Chambers of Commerce, members of Housing Commissions, inspectors of public works, experts of the Italian Naval Register, etc.) and judicial functions (judges, judicial officers, auxiliary bodies of the Administration of Justice such as bankruptcy trustees or liquidators, etc.).

The public function is characterised by the exercise of:

- authoritative power, ie the power that allows the Public Administration to achieve its goals via actual commands, with respect to which private individuals are subjected. This is the activity in which sovereignty is expressed, which includes both the power of coercion (arrest, search, etc.) and of contesting law infringements (ascertaining offences, etc.), as well as the powers of hierarchical supremacy within public offices;
- certification power, ie the power entitling a certifier to attest to a fact that is proving until a complaint of forgery is filed.

The term '**public service**' is related to:

- production activities for goods and services of general interest, subject to the supervision of a Public Authority;
- activities aimed at guaranteeing the rights of the person to life, health, liberty, social security and assistance, education, freedom of communication, etc., under a concession and/or agreement regime.

The subjects representing the Public Administration, performing a public function/service and with whom a direct relationship is established are the 'public officials' or the 'public service officers'.

On the one hand, a **public official** is a person who can form or express the will of the Public Administration or exercise authoritative or certification powers.

By way of example and not limited to, public officials include members of state and territorial administrations, members of supranational administrations (eg the European Union), the Food Law Enforcement Department ('NAS' in Italian), members of Supervisory Authorities, members of Law Enforcement and the 'Guardia di Finanza', members of Chambers of Commerce, administrators of economic public bodies; members of Housing Commissions, judges, judicial officers, auxiliary bodies of the Administration of Justice (eg bankruptcy trustees).

On the other hand, a **public service officer** carries out activities relating to the care of public interests or the satisfaction of needs of general interest subject to the supervision of a public authority. Criminal law has clarified that the bureaucratic classification of the individual within the structure of a public body does not constitute a criterion for recognising the qualification as public service officer; indeed, what is relevant is the activity actually carried out by the individual. Therefore, even a private individual or an employee of a company can be classified as a public service officer when carrying out activities aimed at pursuing a public purpose and protecting a public interest.

By way of example and not limited to, the following are considered to be public service officers: employees of the National Health Service, cashiers of a public body, hospital employees, the Local Health Authority ('ASL' in Italian), the National Institute for Insurance against Accidents at Work ('INAIL' in Italian), the National Institute for Social Security ('INPS' in Italian), employees of municipal energy companies, banks, post offices, customs offices, members of municipal councils, Ferrovie dello Stato employees or Società Autostrade employees.

#### **A1. Sensitive activities in the context of crimes against the Public Administration**

Based on a control and risk self-assessment, the Company has identified the following sensitive and instrumental activities within which crimes against the Public Administration as per arts. 24 and 25 of the Decree might be committed.

A1.1. Management of inspections by the Public Administration, public service officers or certification bodies.

- A1.2. Management of fiscal and tax matters with the Financial Administration, also through external professionals.
- A1.3. Management of relations with the Judicial Authority, also through external professionals.
- A1.4. Management of obligations with the PA as far as authorisations, permits, licenses, waste disposal, etc. are concerned, also through external professionals, as well as during calls for tenders.
- A1.5. Management of regulatory, administrative and corporate obligations (eg filing of powers of attorney, privacy matters).
- A1.6. Request, management and monitoring of subsidised loans, contributions, tax exemptions, social safety nets, employment contributions, training, etc.
- A1.7. Management of financial resources.
- A1.8. Management of consultancy (administrative, fiscal, etc.).
- A1.9. Management of expense reports.
- A1.10. Management of the personnel selection process.
- A1.11. Management of capital goods and corporate benefits (eg cars, mobile phones, personal computers, corporate credit cards, etc.).

## **A2. Specific prevention protocols**

As for the **management of inspections by the Public Administration, public service officers or certification bodies**, the protocols envisage the following:

- the Internal Manager (or a person specifically authorised in writing) shall participate in judicial, tax or administrative inspections;
- the person in charge of the inspection shall inform the Supervisory Body of the start and the end of the proceeding no later than 5 (five) days after its completion, as well as of any critical issues arising during its execution. Copy of the minutes drawn up by the inspection authorities shall be transmitted to the Supervisory Body.

As for the management of fiscal and tax matters with the Financial Administration and the management of relations with the Judicial Authority, also through external professionals, the protocols envisage the following:

- a person in charge must always be identified, in line with the subject matter, with the necessary powers to represent the Company or to coordinate any external professionals;
- the person thus identified shall inform the Supervisory Body of the start of the judicial or tax proceedings, of the results of the various phases of the judgement, of the conclusion of the proceedings, as well as of any critical issues that may be encountered in progress.

As for the management of obligations with the Public Administration as far as authorisations, permits, licenses, waste disposal are concerned and as for the management of regulatory, administrative and corporate obligations, the protocols envisage the following:

- all documents, requests, formal communications and contracts that have the Public Administration as their counterpart shall be managed and signed only by persons with the appropriate powers according to internal regulations.
- The Internal Manager as better identified above (or a person specifically authorised in writing) shall:
  1. Identify the most appropriate tools to ensure that the relationships held by the Company with the Public Administration are always transparent, documented and verifiable;
  2. Authorise in advance the use of data and information regarding the Company and intended for deeds, communications, certificates and requests of any nature whatsoever forwarded/addressed to the Public Administration;
  3. Check that the documents, statements and information transmitted by the Company to have authorisations or permits released are complete and truthful.

As for the request, management, monitoring of subsidised loans, contributions, tax exemptions, social safety nets, employment contributions, training, etc., the protocols envisage the following:

- the Internal Manager as better identified above (or, alternatively, a person specifically

authorised in writing) checks that the statements and documentation submitted to obtain the financing/contribution are complete and represent the real economic, capital and financial situation of the Company;

- the financial resources obtained as a contribution, grant or public financing are intended exclusively for the initiatives and the achievement of the purposes for which they were requested and obtained;
- the requesting party shall always justify the use of such resources and shall certify in writing their coherence with the purposes for which the financing was requested and obtained.

As for the **management of financial resources**, the protocols envisage the following:

- limits to the autonomous use of financial resources, through the definition of quantitative spending thresholds, consistent with management skills and organisational responsibilities; the quantitative spending limits assigned may be exceeded only for proven reasons of urgency and in exceptional cases. In such cases, it is expected that the exceptional event will be regularised by issuing the appropriate authorisations;
- transactions involving the use of economic/financial resources shall be expressly justified, documented and recorded in accordance with the principles of professional and accounting correctness;
- the requesting party shall justify the use of financial resources, even by only stating the type of expenditure to which the transaction belongs;
- no payment or collection may be settled in cash, unless there is express authorisation from the competent function and in any case for amounts that do not exceed sums managed through petty cash payments;
- the Company uses only financial and banking intermediaries subject to transparency and fairness regulations in compliance with European Union legislation;
- quantitative limits on the provision of cash advances and reimbursement of expenses incurred by Company personnel are established in advance, depending on the type of service performed. In particular:

- a. cash advances shall be traceable and appropriately justified;
- b. reimbursement of expenses incurred shall be requested by completing specific forms and only after producing suitable supporting documentation for the expenses incurred.

As for the **management of consultancy**, the protocols envisage the following:

- external consultants are chosen based on professionalism, independence and competence requirements;
- the company function in charge of the selection (or, alternatively, the responsible party) shall always justify the identification of external consultants;
- the appointment of consultants takes place in compliance with the principles of transparency, professionalism and traceability, as well as on the basis of the procedures, authorisations and internal controls adopted by the Company;
- the assignment to external consultants is given in writing. Said document shall contain the agreed payment and the content of the service;
- contracts regulating relationships with consultants shall include specific clauses that refer to the obligations and responsibilities according to the Decree and to the Model; the latter shall be transmitted to them together with the Code of Ethics, as provided for in Section 10 of the General Part;
- the fees or payments due to consultants are paid in an amount that is appropriate to the services provided to the Company, in accordance with the assignment given, the conditions or practices existing on the market, or the professional rates in force for the category concerned;
- contracts regulating relationships with such parties shall include specific clauses stating clear responsibilities in the case of failure to comply with any contractual obligations arising from acceptance of the Code of Ethics and the Model.

As for the **management of expense reports**, the protocols envisage the following:

- depending on the type of business trips, missions or travel outside the usual workplaces, the Internal Manager shall authorise expense reports to the requesting parties *ex ante* or *ex post*;
- expense reports shall be managed according to the methods communicated to all staff regarding compliance with the purposes of the expenses incurred, the forms, the authorisation levels required and the settlement of the sums to be reimbursed.

As for the **personnel selection and hiring process**, the Internal Manager shall:

- Preventively ascertain and evaluate the direct or indirect relationships between the candidate and the Public Administration, evaluating and preventing any future risk situations;
- Promptly inform the Supervisory Body of the candidate's hiring.

As for the **management of capital goods and corporate benefits**, the protocols envisage the following:

- the assignment of the capital goods shall be justified, based on the role and duties of the beneficiary personnel and through a formal request from the interested party;
- the request shall be authorised in writing by the HR manager;
- the assigned capital goods shall be revoked in the event of infringement of company procedures or regulations during their use.



## **B. Cybercrimes**

### **B1. Sensitive activities in the context of cybercrimes**

Based on a control and risk self-assessment, the Company has identified the following sensitive activity within which cybercrimes as per art. 24-bis of the Decree might be committed.

- Management of accesses, accounts and profiles.

### **B2. Specific prevention protocols**

As for the **management of accesses, accounts and profiles**, the protocols envisage the following:

- access to the computer systems shall be guaranteed exclusively via unique authentication of users, namely via user-id and password (for which rules for creation are defined, eg minimum password length, complexity, expiration, etc.);
- a formal authorisation and registration system shall be defined for the assignment, modification and deletion of accounts and their access profiles to systems and applications;
- an application/profile/user matrix shall be set up that is aligned with existing organisational roles and checked periodically;
- formal procedures shall be established for assigning remote access to company systems by employees and managers , as well as third parties such as agents, consultants and suppliers;
- the Company undertakes to formalise the procedures for the assignment and use of special privileges (system administrator, super user, etc.);
- thanks to the proxy system concerning the company network, for each individual user it is possible to recall the name of the person who requested access to the

external network, the time at which this request was forwarded, as well as the paths followed by the same person within the network;

- the Company undertakes to formalise the procedures for the request to, the access to (through identification codes, smart card or other ways) and the methods of use of IT systems belonging to public bodies or public service officers with which the Company interfaces and exchanges data, as well as for assigning responsibility to the individual(s) in possession of the credentials for their use;
- should they use documents signed electronically and/or digitally, the Company undertakes from now on to follow a specific procedure suitable for checking the authenticity of the documents in question. The frequency thereof shall be defined. In this case, the Company shall draft a specific list (checked and updated with a frequency to be defined) containing the names of those persons authorised to sign documents electronically and/or digitally.

## **C. Corporate crimes**

### **C1. Sensitive activities in the context of corporate crimes**

Based on a control and risk self-assessment, the Company has identified the following sensitive and instrumental activities within which corporate crimes as per art. 25-ter of the Decree might be committed.

- Drafting and approval of the financial statements and other corporate documents, also through outsourcers.
- Management of extraordinary transactions.
- Management of relationships with consortium members and the Board of Auditors.
- Management of IT systems.
- Customer assessment activities.
- Management of incoming financial flows.

## C2. Specific prevention protocols

As for the drafting and approval of the financial statements and other company documents, also through outsourcers, the protocols envisage the following:

- an accounting manual (or, alternatively, accounting procedures to be constantly updated) should be adopted where the data and information that each function or organisational unit is to provide, the accounting criteria for processing the data and the timing for their transmission to the responsible functions are clearly indicated;
- all detection and recording of business activities shall be carried out correctly and in compliance with the principles of truthfulness and completeness;
- accounting information suitable for drafting corporate communications shall be collected, transmitted and grouped via methods that guarantee the traceability of the individual steps in the data formation process and the identification of the persons entering the data into the system. The access profiles to this system shall be identified by the person responsible for the IT systems, who guarantees that the functions are separated and the authorisation levels are coherent;
- any changes to the balance sheet items or to their accounting criteria are authorised by the Chairman of the Board of Directors;
- any request by anyone for unjustified changes in the criteria for surveying, recording and accounting representation of or for quantitative changes in data compared to those already accounted for in accordance with the Company's operating procedures shall be immediately notified to the Supervisory Body;
- the drafts of the financial statements and other accounting documents shall be made available to the directors reasonably in advance of the meeting of the Board of Directors called to approve the financial statements;
- if the operations covered by this protocol are outsourced, the Company shall communicate its Code of Ethics and its Model to the service provider, in accordance

with Section 10 of the General Part. Compliance with said documents shall be required through appropriate contractual clauses.

As for the **management of extraordinary transactions**, including those affecting share capital or net worth, the protocols envisage the following:

- each extraordinary transaction shall be submitted to and approved by the Boards of Directors of the entities involved;
- the function proposing the transaction (or the competent function, according to company procedures) shall draft suitable documentation to support said transaction, as well as a preliminary information report illustrating the contents, the underlying interest and the strategic purposes of the transaction;
- where requested, the Board of Statutory Auditors shall express a reasoned opinion on the transaction;
- for the purposes of accounting registration of the transaction, the competent function shall preliminarily check that the documents supporting the transaction are complete, relevant and correct.

As for the **management of relationships with consortium members and the Board of Auditors**, the protocols envisage the following:

- requests and transmissions of data and information, as well as any comments, communications or evaluations expressed by the consortium members and the Board of Auditors, shall be documented and retained;
- all documents relating to transactions on the agenda of the meetings of the Assembly/the Board of Directors (or, in any case, relating to transactions on which the Board of Auditors is required to express an opinion) shall be notified and made available reasonably in advance of the date of the meeting;

- the Board of Auditors and the consortium members shall be given free access to the company accounts and to anything else required for the correct performance of the assignment;
- if the operations covered by this protocol are outsourced, the Company shall communicate its Code of Ethics and its Model to the service provider, in accordance with Section 10 of the General Part. Compliance with said documents shall be required through appropriate contractual clauses.
- As for the **management of IT systems**, the Company has implemented suitable control measures for the prevention of cybercrimes as per Section B) of this Special Part.

As for the **management of customer assessment activities**, the protocols envisage the following:

- when carrying out potentially ‘risky’ or ‘suspicious’ transactions with respect to the standards and principles required by the Decree, customers should be assessed based on the following indicative parameters:
  - √ subjective customer profile (eg questionable reputation; admissions or statements regarding involvement in criminal activity);
  - √ customer behaviour (eg ambiguity, lack of data needed to execute the transactions in question or reluctance to provide them);
  - √ customer's territorial location (eg operations carried out in off-shore countries).
- commercial partners shall be chosen after carrying out suitable checks on their reputation and reliability within the market, as well as after sharing the fundamental ethical principles that guide the Company;
- **contracts regulating relationships with customers shall include specific clauses indicating the latter’s willingness to respect the principles and protocols drawn**

**up within this Model and the Code of Ethics, and in general the postulates established by the Decree.**

As for the **management of incoming financial flows**, the protocols envisage the following:

- for all persons with formal powers to move financial resources, specific limits regarding type of transaction, frequency and amount should be established;
- the joint signature of at least two persons (one of whom has powers of representation) shall be required for transactions above pre-established value thresholds;
- transactions involving the use of economic/financial resources shall be expressly justified, documented and recorded in accordance with the principles of professional correctness and accounting transparency;
- the Company's receipts and payments, as well as cash flows, shall always be traceable and verifiable on the basis of documents;
- the terms and conditions of payment shall be clear, expressed and documented in writing with respect to each individual transaction;

the discount procedure should be defined through clear and timely procedures, drawn up in writing.

**D. Involuntary manslaughter and serious and very serious injuries due to negligence, committed in breach of accident prevention regulations and regulations relating to the protection of hygiene and health at work**

**D1. Premise**

Arts. 589 and 590 para. 3 of the Criminal Code referred to in the Decree punish anyone who causes the death of a person or causes serious or very serious personal injuries due to negligence and has committed such crimes by violating the accident

prevention regulations and those relating to the protection of hygiene and health at work.

**‘Injury’** means the set of pathological effects constituting illness, ie those organic and functional alterations resulting from the occurrence of violent conduct.

An injury is defined as ‘serious’ if the disease has endangered the victim's life, has caused a convalescence period of more than forty days or has led to the permanent weakening of the functional potential of a sense (eg hearing) or of an organ (eg the dental apparatus).

It is defined as ‘very serious’ if the conduct has caused a probably incurable disease (ie with permanent, incurable effects) or the total loss of a sense, a limb, the ability to speak correctly or to procreate or the use of an organ or if it has deformed or disfigured the victim's face.

Whether it is a serious/very serious injury or death, a **harmful event** can be perpetrated through either active behaviour (the agent carries out a conduct with which he/she harms the integrity of another individual) or an omission (the agent simply does not intervene to prevent the harmful event). By way of example, active conduct will be found in an employed person who directly carries out operational tasks and materially damages others, whereas omission will usually be found in senior personnel who do not comply with the supervision and control obligations and thus do not intervene to prevent the event caused by others.

From a **subjective standpoint**, manslaughter or injuries relevant for the purposes of the administrative liability of the entities must be due to negligence: this subjective charge can be general (breach of rules of conduct crystallised in the social fabric under the rules of experience based on the parameters of diligence, prudence and expertise) or specific (breach of rules of conduct originally deriving from rules of experience and later come into existence in laws, regulations or orders).

A profound difference exists in this compared to the subjective attribution criteria provided for the other crime cases referred to in the Decree, all punished on the basis

of malice, ie when the individual is fully aware and wilful when carrying out said actions and they are thus not due to mere guilt.

With regard to the omission, it is specified that an individual is liable for his/her own negligent omission (which is harmful to the life or physical safety of a person) only if he/she holds a position of guarantee towards the victim, which may originate from a contract or from the unilateral will of the agent. The rules identify the employer<sup>5</sup> as the guarantor of ‘the physical integrity and moral personality of the workers’; said position as guarantor is in any case transferable to other individuals, provided that the relative delegation is sufficiently specific, drafted in writing on a deed and suitable for transferring all the authoritative and decision-making powers necessary to protect the safety of employed persons. Furthermore, the person chosen to fill the position must be capable and competent in the matter addressed by the transfer of responsibility.

According to the new regulations introduced by the legislator, the harmful conduct of the agent must necessarily be aggravated for it to be attributed to the entity; in other words, it must originate from the breach of accident prevention regulations concerning the protection of hygiene and health at work. For the purposes of implementing the Model, it is necessary to consider the following:

- Compliance with the minimum safety standards laid down in the sector-specific regulations does not exhaust the overall duty of care required (specific fault).
- It is necessary to ensure the adoption of safety standards such as to minimise (and, if possible, eliminate) any risk of injury or illness, also based on the best known technique and science, according to the particularities of the work (general fault).
- For the purposes of the Model, the conduct of the injured worker who gave rise to the event does not exclude all liability on the part of the entity when the event is in any case attributable to the lack/insufficiency of precautions (which, if adopted, would have neutralised the risk underlying such conduct). The prevention obligation

---

<sup>5</sup> In compliance with art. 2, para. 1 b) of Legislative Decree No 81/08, the employer is the party holding the relevant employment relationship with workers or, in any case, the party who, according to the type and structure of the organisation within which workers carry out their activity, has responsibility for the organisation itself or for the production unit as he/she exercises the decision-making and spending powers (art. 2, para. 1 of Legislative Decree No 81/08).



is excluded only if a worker's behaviour is exceptional, abnormal or excessive in relation to the work procedure, the organisational directives received and common prudence.

As far as the protected individuals are concerned, the accident prevention regulations are meant to protect both employees and all persons who legitimately enter the premises used for carrying out work.

As far as active persons are concerned, the types of crimes referred hereto may be committed by whoever carries out sensitive activities in the matter by virtue of their role. Examples:

- a worker who, through his/her actions and/or omissions, may jeopardise his/her own and others' health and safety;
- the manager and the supervisor, who may be responsible for, among other things, coordination and supervision of activities, training and information;
- the employer as the main actor in the field of prevention and protection.

**D2. Sensitive activities in the context of the crimes of involuntary manslaughter and serious and very serious injuries due to negligence, committed in breach of accident prevention regulations and regulations relating to the protection of hygiene and health at work**

Sensitive activities in which the crimes of involuntary manslaughter and serious or very serious injuries due to negligence might be committed while breaching the accident prevention regulations and those regarding health and hygiene at work provided for by art. 25-septies of the Decree have been classified as follows:

- activities at risk of injury and occupational disease;
- activities at risk of crime.

This dichotomous classification arises from the fact that the former are the activities within which accidents may occur, whereas the latter are those within which

the crime can be committed by members of the organisation for negligent breach of the regulations and existing prevention measures to protect health, hygiene and safety at work.

### **D2.1 Activities at risk of injury and occupational disease**

The activities within which injuries or occupational diseases may occur are taken from the Risk Assessment Sheet ('Documento di Valutazione dei Rischi' in Italian, hereinafter 'DVR'); by conducting careful investigations involving both structural and organisational aspects, the Company has identified the risks to the workers' safety and health. The document also points out the protection measures aimed at their elimination or containment.

For each risk category in the DVR, all the dangers that are actually applicable are mentioned and appropriately coded.

The Risk Assessment Sheet is constantly updated in the light of new and possible prevention needs, according to the procedures set out in the Model.

### **D2.2 Activities at risk of crime**

The activities whose omission or ineffective implementation could constitute involuntary liability for the Company following an event of involuntary manslaughter or serious/very serious injuries caused are reported below. A brief description of their content is also provided.

- Risk assessment: management of the activities regarding the execution and the updating of the risk assessment, carried out for the purposes of the legislation in force, in terms of health, hygiene and accidents in the workplace, also with the help of consultants external to the Company who are experts in these issues; management of the activities regarding the updating of the control devices and the related procedures, defined in light of the risk assessment; management of the

activities regarding the drafting of the Risk Assessment Sheet and the documents connected to it in compliance with the legislation in force in terms of health, hygiene and accidents in the workplace and at any temporary or mobile construction sites.

- Appointments and definition of responsibilities: assignment of 'sensitive' responsibilities in matters of health and safety at work without prior verification of the requirements.
- Health surveillance: management of activities aimed at ensuring the implementation of the health surveillance required for each job category.
- Training: management of activities aimed at offering an adequate (in terms of time and topics covered) training, information and instruction programme to all employed persons and in particular to those who carry out higher-risk activities; management of activities aimed at providing an adequate level of knowledge to the RSSP and to other possible figures such as the works manager, the coordinator at the design stage and the coordinator at the execution stage, when coinciding with figures within the Company, on the issues governed by the reference legislation on health, hygiene and accidents in the workplace.
- Assignment of work to external parties: management of verification activities and those relating to the preparation, evaluation and awarding of tenders; management of verification activities on the costs incurred to make the Risk Assessment Sheet and the safety plans operational, so that they can guarantee the maximum level of safety in the workplace and at any temporary or mobile construction sites.
- Purchases: supplier management; purchases of products, equipment, machinery and systems with the necessary requirements in terms of applicable laws and regulations.
- Maintenance: management of maintenance activities regarding workplaces, equipment, vehicles, machinery and systems used, in order to limit possible accidents caused by them.

- Special risks: management of constant verification activities at workplaces regarding compliance with the provisions of current legislation.
- Emergencies: emergency management.
- Procedures and work instructions: management of activities regarding the preparation and implementation of company procedures and related control measures in line with current legislation on health, hygiene and accidents in the workplace, as well as constant updating of said procedures in the event of changes to the aforementioned legislation; application of work procedures and operating instructions.
- Communication and staff involvement: non-conformity management; corrective and preventive actions.

The list of sensitive activities is periodically updated in the light of new and possible prevention needs, according to the procedures set out in the Model.

## **F.1 General principles of conduct**

In addition to what is provided for in Section 2 of the Special Part, further general principles of conduct apply.

The Model does not intend to replace the legal prerogatives and responsibilities governed by the persons identified by the Legislative Decree No 81/08 and by the legislation further applicable in specific cases. On the contrary, it serves as an additional means of control and verification of the existence, effectiveness and adequacy of the structure and organisation put in place in compliance with the specific legislation in force regarding accident prevention, safety and health protection in the workplace.

One of the Model's assumptions for the prevention of accidents at work envisage that the Company's workers and any external persons who are legitimately present at the Company's premises respect certain principles and behave in a certain way.

In particular, each worker, each individual and more generally each recipient of the Model who is legitimately employed by the Company shall:

- In accordance with their training and experience, as well as the instructions and means provided or arranged by the employer, not adopt imprudent behaviour with regard to safeguarding their health and safety;
- Comply with internal company regulations and procedures for the purpose of collective and individual protection, in particular by exercising all appropriate controls and activities suitable for safeguarding the health and safety of external collaborators and/or outsiders who may be present in the workplace;
- Correctly use machinery, equipment, tools, dangerous substances, materials and preparations, means of transport and other work equipment, as well as the safety and protection devices made available;
- Immediately report to the appropriate functions (in accordance with the responsibilities assigned) any anomalies in the means and devices referred to in the previous points, as well as any other dangerous conditions of which they become aware;
- Take action directly when faced with a detected danger and only in cases of urgency, consistent with one's own skills and possibilities;
- Undergo the required health checks;
- Undergo the required training interventions;
- Contribute to the fulfilment of all obligations imposed by the competent authority or otherwise necessary to protect the safety and health of workers at work.

For these purposes, it is prohibited to:

- Remove or modify safety, signalling or control devices without authorisation;

- Carry out on one's own initiative operations or manoeuvres that are not within one's competence or that may compromise one's own safety or that of other workers.

#### **D4. General prevention protocols**

In addition to what is provided for in Section 3 of the Special Part, further general prevention protocols apply.

The Risk Assessment Sheet envisages specific measures for the prevention of accidents and occupational diseases. For details thereof, please refer entirely to the job description sheets supplementing the DVR.

As regards the preventive measures for activities at risk of crime, as identified above, or those behaviours that could constitute the Company's fault in relation to accidents at work, the Organisation, Management and Control Model is adopted and implemented in order to guarantee the fulfilment of all legal obligations relating to the following:

- compliance with the technical-structural standards of law relating to equipment, systems, workplaces, chemical, physical and biological agents;
- risk assessment activities and preparation of the resulting prevention and protection measures;
- organisational activities, such as emergencies, first aid, contract management, periodic safety meetings, consultations with workers' safety representatives;
- health surveillance activities;
- information and training activities for workers;
- supervisory activities with reference to compliance with safety work procedures and instructions by workers;
- acquisition of legally required documents and certifications;
- periodic checks on the implementation and effectiveness of the procedures adopted;

- where applicable, the necessary communications to the competent authorities.

For the purposes of maintaining the Organisation, Management and Control Model, it is necessary to provide evidence of what has been implemented; this is done by resorting to appropriate recording systems.

It is also important to ensure that both internal and external documents (eg documents relating to products and substances, documents certifying the conformity of machines) are constantly available and updated. The management of both internal/external documents and records constituting special documents is such as to guarantee their traceability, conservation and updating.

Compliance with current legislation (laws, technical standards and regulations, etc.) is guaranteed by:

- identification and accessibility of the relevant regulations applicable to the Company;
- continuous updating of the regulations applicable to the Company's activities;
- periodic monitoring of compliance with applicable regulations.

For the purposes of adopting and implementing the Organisation, Management and Control Model, the Company also undertakes to implement the specific protocols indicated below.

#### **D5. Specific prevention protocols**

Below are the specific prevention protocols within each sensitive area (ie at risk of crime) identified and assessed through the control and risk self-assessment carried out by the Company. Each area is regulated by a specific operating procedure.

#### **Risk assessment.**

Since risk assessment represents the cornerstone for ensuring the health and safety of workers and is also the main tool for identifying the consequent protection measures (whether aimed at reducing or eliminating the risk), the risk identification and detection should be carried out correctly and in compliance with the principle of truthfulness, completeness and accuracy. The legislation currently identifies the employer as the competent person for the assessment; he/she can rely on other persons (such as the person in charge of the prevention and protection service and the company doctor) for that and always consults the workers' safety representative beforehand.

All data and information useful for risk assessment and consequently for the identification of protection measures (eg technical documents, instrumental measures, results of internal surveys, etc.) must be clear and complete and must truthfully represent the state of the art of the Company.

The data and information are collected and processed promptly under the supervision of the employer, who may also engage persons in possession of suitable requirements as to technical expertise and, if necessary, instrumental expertise; said expertise must be certifiable in the cases provided for.

Upon request, any documents and sources from which the information is taken must also be transmitted together with said data and information.

The drafting of the Risk Assessment Sheet and the Prevention and Protection Measures Plan cannot be delegated by the employer. Furthermore, it must be carried out on the basis of the preliminarily defined criteria (which integrate said documents); the risk assessment criteria include, among others, the following points:

- routine and non-routine activities;
- activities of all persons having access to the workplace (including outsiders);
- human behaviour.
- dangers coming from outside;



- hazards related to the work or arising in the surrounding environment;
- infrastructure, equipment and materials at the workplace;
- changes made to processes and/or the management system, including temporary changes, and their impact on operations, processes and activities;
- any applicable legal obligations regarding risk assessment and implementation of necessary control measures;
- design of work environments, machinery and systems;
- operational and work procedures.

### **Appointments and definition of responsibilities**

For all the figures identified for the management of issues relating to health and safety in the workplace, technical-professional requirements are defined which may also originate from specific regulatory provisions. Each of these figures must possess these requirements before the task is assigned and must maintain them over time; said requirements can also be achieved via specific training.

Specific responsibilities in matters of health and safety are assigned in writing, clearly stating a starting/ending date, exhaustively defining the characteristics and limits of the assignment and, if applicable, identifying the spending power.

In order to ensure that the responsibilities related to company roles and functions are assigned effectively:

- the management, coordination and control responsibilities within the Company are adequately formalised;
- the persons envisaged by the legislation on matters of hygiene and safety in the workplace are correctly appointed (including, in the case of construction sites, the persons envisaged by Title IV of Legislative Decree No 81/08) and are correctly granted the powers necessary to carry out the role assigned to them;

- The system of delegations, signature and spending powers is consistent with the assigned responsibilities;
- the assignment and exercise of powers within a decision-making process are consistent with positions of responsibility and with the relevance and/or criticality of the underlying risk situations;
- there is no subjective identity between those who make or implement decisions, those who must provide accounting evidence of them and those who are required to carry out the checks as per the law and the procedures contemplated by the internal control system;
- the persons in charge (and/or appointed pursuant to the legislation in force) of hygiene and safety in the workplace possess adequate and effective skills in the matter.

### **Health surveillance**

Prior to assigning any task to a worker, it is necessary to check his/her requirements, both with regard to technical aspects (see the next sensitive activity: **Training**) and with regard to health aspects, based on what emerges from the risk assessment.

The suitability check is carried out by the company doctor: based on the indications provided by the employer and on his/her own knowledge of the workplace and the processes, he/she verifies in advance the health suitability of the worker by issuing judgements of total or partial suitability or unsuitability for the job. Depending on the type of work required and on the results of the preliminary visit, the company doctor defines a health surveillance protocol for the workers;

said protocol is periodically updated based on new legislative requirements, changes in activities and processes, identification of new risks to workers' health.

## Training

All personnel receive appropriate information on the correct procedures for carrying out their duties, are adequately trained and, where required by law, are instructed. Said training and/or instruction shall be properly documented. Training activities are provided via numerous methods (eg face-to-face training, written communications, etc.) defined both by the Company's choices and by current legislation requirements.

The choice of the training body may be limited by specific regulatory provisions.

The documents relating to staff training is sent to the HR manager and is also used for the purpose of assigning new tasks.

The training activity aims to:

- Ensure (including through appropriate planning) that any person under the control of the organisation is competent in the light of appropriate education, training or experience;
- Identify training needs related to the performance of the activities and provide due training or consider other actions to meet these needs with the same effectiveness;
- Evaluate the effectiveness of training activities or other actions implemented, and keep related records;
- Ensure that the personnel are aware of the actual/potential impact of their work, the correct behaviours to adopt and their roles and responsibilities.

Furthermore, once the training activity has been duly completed, the Company shall adopt appropriate means (if necessary, also financial means) to guarantee the participation of workers (also through their own representatives). This shall be done by:

- Involving them in identifying hazards, assessing risks and defining protective measures;

- Involving them in the investigation of an accident;
- Consulting them when changes are planned that are likely to have significant effects on health and safety matters.

### **Outsourcing of work to external parties**

Contracted activities and work performances are governed by art. 26 and Title IV of the Legislative Decree No 81/08. The entity carrying out the work shall possess suitable technical-professional requirements, also verified through registration with the Chamber of Commerce. Said entity shall prove compliance with insurance and social security obligations towards its staff, including through the submission of the single document certifying payment of contributions ('Documento Unico di Regolarità Contributiva' in Italian - DURC for short). If necessary, the entity carrying out the work shall also submit to INAIL a specific report for any total or partial changes to the activity already insured (based on the type of intervention requested and on the information provided by the Company).

In the cases provided for by law, at the end of the interventions the entity shall issue the Declaration of Conformity to the state of the art.

Furthermore, safety and coordination plans shall be adequate and effectively implemented in the case construction sites are in place.

### **Purchases**

Equipment, machinery and systems shall be purchased after evaluating their health and safety requirements, also taking into account the considerations of workers through their representatives.

Equipment, machinery and systems shall comply with the current legislation provisions (eg CE marking, DoC issued by the installer, etc.). Where applicable, in

accordance with the applicable legislative provisions, their entry into service shall be subject to initial examination or approval procedures.

Before using new equipment, machinery or systems, the worker in charge shall be trained and/or instructed appropriately.

Purchasing is managed in such a way that:

- The criteria and methods for qualifying and verifying supplier requirements are defined;
- The procedures for verifying the compliance of the equipment, systems and machinery to be purchased with current regulations (eg CE marking) and the criteria and procedures for assessing the compliance of health and safety requirements, also providing for consultation of workers' representatives, are defined;
- Where applicable, the methods for carrying out acceptance checks, initial checks and approvals required for commissioning are provided.

## **Maintenance**

All equipment, machinery and systems that may have significant impacts on health and safety are subject to scheduled maintenance protocols, with timing and methods also defined by the manufacturers. Any specialist interventions are conducted by persons in possession of the legal requirements; this shall be proven via the necessary documents.

Maintenance activities on safety devices are subject to recording.

If equipment and systems are in place for which current legislation requires periodic verification conducted by specific external bodies (eg ARPA, ASL, Notified Bodies, Inspection Bodies, etc.), a specific verification contract shall be stipulated with the relevant body. If no service is provided within the time frames set by the legislation, the following procedure shall be followed:

- in the event of additional persons in possession of the qualifications/authorisations to carry out the verification, the task shall be assigned to them;
- if no alternative persons exist, self-diagnosis shall be carried out through existing technical structures on the market (eg maintenance companies, engineering consortia, etc.).

Maintenance is managed in such a way that:

- Methods, time frames and responsibilities for the planning and carrying out of maintenance and periodic verification, where required, of equipment, systems and machinery (identified promptly in specific protocols/sheets) and the periodic monitoring of their efficiency are defined;
- Performed maintenance activities and related responsibilities are recorded;
- Methods for reporting anomalies are defined and the most suitable means for communicating such methods and the functions required to activate the relative maintenance process (unscheduled maintenance) are identified.

### **Special risks**

Workplaces shall also be designed in compliance with ergonomic, comfort and well-being principles. They shall undergo regular maintenance so that defects that may affect the safety and health of workers are eliminated as quickly as possible; adequate hygienic conditions shall be ensured.

Any areas under a specific risk shall be appropriately marked and, where appropriate, made accessible only to adequately trained and protected individuals.

### **Emergencies**

Escape routes shall be identified and care shall be taken to keep them efficient and free from obstacles. Staff shall be made aware of emergency reporting and management procedures.

A sufficient number of emergency response personnel shall be identified and trained in advance according to legal requirements.

Suitable types and adequate numbers of fire-fighting systems shall be in place and maintained efficiently; their choice shall be based on either the specific fire risk assessment or the indications provided by the competent authority. Suitable medical facilities shall also be in place and maintained in good working order.

Emergency management shall be implemented through specific plans that envisage the following:

- identifying situations that may cause a potential emergency;
- definition of suitable methods to respond effectively to any emergencies and to prevent/mitigate their negative consequences on health and safety;
- planning for verification of the effectiveness of emergency management plans;
- updating of emergency procedures in the event of accidents or negative outcomes of periodic simulations.

### **Work procedures and instructions**

Due to the nature of the Company's activities, specific work instructions or operating procedures may be provided; these shall be accessible to all workers, together with the documents on the methods of use of machinery and equipment and the safety documents of the substances.

### **Communication and staff involvement**

For the purposes of health and safety in the workplace, the Company shall adopt suitable means aimed at ensuring the following:

- internal communication between the various levels and functions in the organisation;
- communication with suppliers and other visitors to the workplace;
- receiving and responding to communications from external interested parties;
- participation of workers (including through their own representatives) by:
  - Involving them in identifying hazards, assessing risks and defining protective measures;
  - Involving them in the investigation of an accident;
  - Consulting them when changes are planned that are likely to have significant effects on health and safety matters.

#### **D6. Further prevention protocols**

Pursuant to the Model, specific controls shall be established to ensure that the Company's organisational system (defined in accordance with the applicable regulations on safety at work and accident prevention) is constantly monitored and placed in the best possible operating conditions.

For the purposes of monitoring the implementation of what is envisaged in Section D5, specific audit activities shall be conducted, also with the collaboration of competent company individuals and possibly external consultants.



**E. Receiving stolen goods, laundering, use of money, goods or benefits of illicit origin and self-laundering; crimes relating to payment instruments other than cash and fraudulent transfer of values**

**E1. Sensitive activities in the context of crimes of receiving stolen goods, laundering, use of money, goods or benefits of illicit origin and self-laundering**

Based on a control and risk self-assessment, the Company has identified the following sensitive activities within which crimes of receiving stolen goods, laundering and use of money, goods or utilities of illicit origin as per art. art. 25-octies of the Decree might be committed.

- Provider evaluation and purchase of functional products for one's business, as well as of goods or benefits.
- Customer evaluation and showcase of finished products, goods and services.
- Management of incoming and outgoing financial flows, including the use of payment instruments other than cash (cashless).

**E2. Specific prevention protocols**

As for the evaluation of providers and customers; the purchase of finished products, goods and services; and the showcase of finished products, goods and services, the protocols envisage the following:

- when carrying out potentially 'risky' or 'suspicious' transactions with respect to the standards and principles required by the Decree, suppliers and customers should be assessed based on the following indicative parameters:
  - √ subjective profile of the counterparty (eg questionable reputation; admissions or statements of the counterparty regarding involvement in criminal activity);
  - √ counterparty behaviour (eg ambiguity, lack of data needed to execute the transactions in question or reluctance to provide them);

- √ counterparty's territorial location (eg operations carried out in off-shore countries);
- √ economic and financial profile of the transaction (eg unusual transactions in terms of type, frequency, timing, amount, geographical location);
- √ features and purpose of the transaction (eg use of nominees, changes to the standard contractual conditions , purpose);
- √ commercial partners shall be chosen after carrying out suitable checks on their reputation and reliability within the market, as well as after sharing the fundamental ethical principles that guide the Company;
- √ contracts regulating relationships with providers and customers shall include specific clauses indicating the latter's willingness to respect the principles and protocols drawn up within this Model and the Code of Ethics, and in general the postulates established by the Decree.

As for the **management of incoming and outgoing financial flows**, including the use of payment instruments other than cash (cashless), the protocols envisage the following:

- specific limits should be established for all persons with formal powers to move financial resources, based on the type, frequency and amount of the transaction; furthermore, the joint signature of at least two persons is required for transactions above certain pre-established value thresholds;
- for the management of incoming and outgoing flows, only the channels of banks and other financial intermediaries accredited and subject to the discipline of the European Union or credit/financial institutions located in a non-EU country shall be used, which impose obligations equivalent to those provided for by the laws on laundering and provide for the control of compliance with such obligations;
- for the management of incoming and outgoing flows that involve the use of payment instruments other than cash, ownership of the instruments as well as their

legitimate origin and lawful use shall be guaranteed;

- both incoming and outgoing cash flows are prohibited, except for minimum types of expenditure expressly authorised by the Chairman of the Board of Directors or the General Manager, and in particular for petty cash transactions;
- transactions involving the use of economic/financial resources shall be expressly justified, documented and recorded in accordance with the principles of professional correctness and accounting transparency;
- the Company's receipts and payments, as well as cash flows, shall always be traceable and verifiable on the basis of documents;
- transactions capable of altering, forging or tampering with credit cards, payment cards or other payment instruments other than cash or altering in any way the functioning of a computer or telecommunication system are prohibited if the act results in a transfer of monetary value;
- all transactions that involve the possibility of fictitiously attributing ownership/availability of SCF money in order to evade the provisions of the law regarding patrimonial prevention measures or to facilitate the commission of crimes of receiving stolen goods, laundering or use of money or other benefits of illicit origin are prohibited;
- the creation of separate assets and/or assets intended for a specific business outside of cases of actual business necessity is prohibited.

## **F. Crimes relating to copyright infringement**

### **F1. Sensitive activities in the context of crimes of copyright infringement**

Based on a control and risk self-assessment, the Company has identified the following sensitive activities within which some of the crimes relating to copyright infringement as per art. 25-novies of the Decree might be committed.

Purchase, management and dissemination of protected intellectual works.

## **F2. Specific prevention protocols**

For operations concerning the activity in question, the specific protocols envisage the following:

- suitable criteria and methods should be defined and implemented to control the purchase and use of copyrighted goods and software formally authorised and certified;
- periodic checks on installed software are expected to detect if prohibited and/or unlicensed and/or potentially harmful is in place;
- the documents regarding each individual activity should be archived in order to guarantee its complete traceability;
- the criteria and methods for assigning, modifying and deleting user profiles should be defined.

## **G. Inducement not to make statements or to make false statements to the Judicial Authority**

### **G1. Sensitive activities in the field of inducement not to make statements or to make false statements to the Judicial Authority**

Based on a control and risk self-assessment, the Company has identified the following sensitive activities within which the crime of inducement not to make statements or to make false statements to the Judicial Authority as per art. 25-nonies of the Decree might be committed.

Management of relationships with individuals who have the right to remain silent in legal proceedings.

## **G2. Specific prevention protocols**

For operations concerning the activity in question, the specific protocols envisage the following:

- all recipients of the Model shall make use of practices and behave in such a way as to respect the Code of Conduct adopted by the Company.

## **H. Employment of third-country nationals whose stay is irregular**

### **H1. Sensitive activities in the context of crimes relating to the employment of third-country nationals whose stay is irregular**

Based on a control and risk self-assessment, the Company has identified the following sensitive activities within which the crime of employing third-country nationals whose stay in Italy is irregular as per art. 25-duodecies of the Decree might be committed.

Procedures for hiring new staff and/or assigning tasks to third-country nationals.

### **H2. Specific prevention protocols**

For operations concerning the activity in question, special and cogent attention shall be paid when hiring and/or assigning tasks to foreign citizens, as well as to the candidates' identity documents and residence permits.

## **I. Racism and xenophobia crimes**

### **I1. Sensitive activities in the context of crimes relating to racism and xenophobia**

Based on a control and risk self-assessment, the Company has identified the following sensitive activities within which some of the crimes relating to racism and xenophobia as per art. 25-terdecies of the Decree might be committed.

Licence negotiation and management.

### **I2. Specific prevention protocols**

For operations concerning the activity in question, the specific protocols envisage the following:

- all recipients of the Model shall make use of practices and behave in such a way as to respect the Code of Conduct adopted by the Company, with particular reference to its ethical principles;
- when negotiating licences, agreements, etc., great attention shall be paid to not engaging in or having racial, ethnic or religious discriminatory behaviour.

## **J. Tax crimes**

### **L1 Sensitive activities in the context of tax crimes**

Based on a control and risk self-assessment, the Company has identified the following sensitive activities within which tax crimes as per art. 25-quinquiesdecies of the Decree (fraudulent declaration through the use of invoices or other documents for non-existent transactions - fraudulent declaration through other artifices - issuing invoices or other documents for non-existent transactions - concealment or destruction of accounting documents - fraudulent evasion of payment of taxes - failure to declare, incorrect declaration, undue compensation if committed even in part in another European Member State for the purpose of evading VAT for amounts not less than €10 million) might be committed.

Administrative-financial process (management of financial flows, management of active and passive cycles, registration, drafting and storage of accounting and extra-accounting documents, tax calculation and tax compliance), information system management process.

### **L2 Specific prevention protocols**

For operations concerning the activity in question, the specific protocols envisage the following:

the financial administrative functions pay particular attention to and supervise the recording and issuing of invoices via the electronic invoicing system, the relationships with tax consultants and the entity in charge of the legal auditing of accounts, the procedures for identifying and calculating taxable amounts and related taxes, as well as the conservation and custody of accounting records.

Finally, as far as **tax obligations** are concerned, it is forbidden to:

- Omit data and information required by law on the Company's economic, asset and financial situation;
- Breach, evade or avoid tax declaration, attestation or certification obligations provided for by law;
- Fail to comply with legal requirements regarding accounting, corporate information, asset valuation and drafting of financial statements;
- Conceal in accounting income subject to taxation, falsely represent non-real expenses, issue invoices for non-existent services, make estimates and evaluations and determine balance sheet items with methods and evaluation criteria different from those required by law;
- Behave so as to materially prevent the control bodies from performing control and audit activities by concealing documents or using other fraudulent means, or in any other way hinder them in the process;
- Hinder, in any way whatsoever, the carrying out of checks, assessments and inspections by Sector, Tax or Judicial Authorities;
- Destroy or lose accounting documents;
- Sell or carry out other fraudulent acts on one's own or other people's assets which are likely to make the compulsory collection procedure ineffective, whether in whole or in part;
- State assets in the documentation submitted for the purposes of the tax transaction procedure for an amount lower than the actual amount or state fictitious liabilities for a total amount greater than € 5,000.

The administrative-accounting functions collaborate with the IT functions in managing the archiving of company documentation, accounting records and mandatory tax records, in managing electronic invoicing and back-ups of the accounting archive, with provision for adequate IT security systems and adequate access authorisation systems.

