



**Fondazione Generali - The Human Safety
Net ONLUS**

**ORGANISATION AND MANAGEMENT
MODEL AS PER LEGISLATIVE
DECREE 231/01**

generali.com



CONTENTS

Definitions.....	5
GENERAL PART	8
Foreword.....	8
1 The Organisation and Management Model of Fondazione Generali - The Human Safety Net ONLUS	9
1.1 Governance Model of the Foundation.....	9
1.2 The System of Internal Controls	9
1.3 Construction of the Model	10
1.4 Structure of the Model.....	10
1.5 Addressees of the Model	12
2 Components of the Organisation and Management Model.....	13
2.1 Code of Conduct.....	13
2.2 Organisational System.....	13
2.3 Remuneration and incentive scheme.....	13
2.4 Outsourced processes	14
2.5 System of powers	14
2.6 Internal Regulatory system	14
2.7 Management control and control of financial flows	14
2.8 Control safeguards as per Legislative Decree 231/2001	15
2.9 Plan for Disseminating the Model and for the relevant Training of Staff	16
3 Surveillance Body.....	16
3.1 The Surveillance Body of Fondazione Generali – The Human Safety Net ONLUS	16
3.2 Duties and powers of the Surveillance Body.....	18
4 Penalty System	21
4.1 Functions of the Disciplinary and Penalty System	21
4.2 Disciplinary offences and sanctions.....	21
5 Update and Adaptation of the Model.....	23
SPECIAL PART	25
Foreword.....	25
How to read the Special Part.....	25
SECTION A – OFFENCES AGAINST THE PUBLIC ADMINISTRATION AND PRIVATE-TO-PRIVATE CORRUPTION	28

Internal

A 1. Introduction	28
A 2. Relevant offences for the Foundation	29
A 3. Identification of sensitive activities	31
A 4. General principles of conduct	52
A 5. Specific control principles for sensitive activities.....	54
A 6. Further Control Safeguards	57
SECTION B – COMPUTER CRIMES	59
B 1. Relevant offences for the Foundation	59
B 2. Identification of sensitive activities	60
B 3. General principles of conduct	66
B 4. Specific control principles for sensitive activities.....	66
SECTION C – ORGANISED CRIME AND TRANSNATIONAL OFFENCES.....	67
C 1. Relevant offences for the Foundation	67
C 2. Identification of sensitive activities	67
C 3. General principles of conduct	70
C 4. Specific control principles for sensitive activities.....	71
C 5. Further Control Safeguards	72
SECTION D - CRIMES OF COUNTERFEITING OF CURRENCY, LEGAL TENDER, REVENUE STAMPS, AND DISTINCTIVE SIGNS.....	73
D 1. Relevant offences for the Foundation	73
D 2. Identification of sensitive activities	73
D 3. General principles of conduct	75
D 4. Specific control principles for sensitive activities.....	75
D 5. Further Control Safeguards	76
SECTION E – CORPORATE OFFENCES.....	77
E 1. Relevant offences for the Foundation	77
E 2. Identification of sensitive activities	77
E 3. General principles of conduct	81
E 4. Specific control principles for sensitive activities.....	82
E 5. Further Control Safeguards	84
SECTION F – MANSLAUGHTER AND SERIOUS OR VERY SERIOUS INJURIES COMMITTED IN VIOLATION OF THE LAWS ON PROTECTION OF HEALTH AND SAFETY IN THE WORKPLACE	85
F 1. Introduction	85
F 2. Relevant offences for the Foundation	85
F 3. Identification of sensitive activities	86

F 4. General principles of conduct	90
F 5. The organisational structure regarding health and safety at work.....	91
F 6. Specific control principles for sensitive activities.....	91
F 7. Further Control Safeguards	97
F 8. The Verification and Control Model.....	98
SECTION G – CRIMES OF HANDLING STOLEN GOODS, MONEY-LAUNDERING AND USING MONEY, GOODS OR ASSETS OF UNLAWFUL ORIGIN, AS WELL AS SELF-LAUNDERING AND CRIMES OF TERRORISM AND SUBVERSION OF THE DEMOCRATIC ORDER	101
G 1. Relevant offences for the Foundation	101
G 2. Identification of sensitive activities	101
G 3. General principles of conduct	105
G 4. Specific control principles for sensitive activities.....	105
G 5. Further Control Safeguards	107
SECTION H - COPYRIGHT VIOLATIONS	108
H 1. Relevant offences for the Foundation	108
H 2. Identification of sensitive activities	108
H 3. General principles of conduct	110
H 4. Specific control principles for sensitive activities.....	110
H 5. Further Control Safeguards	110
SECTION I – INSTIGATION NOT TO TESTIFY OR TO GIVE FALSE TESTIMONY BEFORE COURT AUTHORITIES	111
I 1. Relevant offences for the Foundation	111
I 2. Identification of sensitive activities	111
I 3. General principles of conduct	112
I 4. Specific control principles for sensitive activities.....	112
I 5. Further Control Safeguards	112
SECTION J – ENVIRONMENTAL CRIMES	113
J 1. Relevant offences for the Foundation	113
J 2. Identification of sensitive activities	114
J 3. General principles of conduct	117
J 4. Specific control principles for sensitive activities.....	118
J 5. Further Control Safeguards	121
SECTION K – EMPLOYMENT OF FOREIGN NATIONALS WITH IRREGULAR RESIDENCE PERMITS, ILLICIT BROKERING AND LABOUR EXPLOITATION	122
K 1. Relevant offences for the Foundation	122
K 2. Identification of sensitive activities	122

K 3. General principles of conduct	124
K 4. Specific control principles for sensitive activities.....	124
K 5. Further Control Safeguards	125

Definitions

Sensitive activities	Activities of the Foundation that are exposed to the – either potential or real – risk that the offences referred to in the Decree might be committed.
Instrumental activities	Activities/processes of the Foundation that are potentially instrumental in committing the offences referred to in the Decree.
Independent Supervisory Authorities	Data Protection Supervisor (<i>Garante Privacy</i>), Authority for Fair Competition (Antitrust Authority), Public Work Supervisory Authority, etc.
Data Protection Supervisory Authority	The Data Protection Supervisor is an independent administrative authority set up by the Italian privacy law (Law no. 675 of 31 December 1996), which transposed EU Directive 95/46/EC into Italian law, authority which today is regulated by the Data Protection Code (Legislative Decree no. 196 of 30 June 2003).
Collaborators	Subjects who collaborate with the organisation in various capacities (e.g. external lawyers).
Consultants	Parties acting in the name and/or on behalf of Fondazione Generali - The Human Safety Net ONLUS by virtue of a contract or mandate.
Outsourcing contract	Agreement whereby a party (called outsourcee or principal) transfers to another party (called outsourcer) some functions needed to achieve the business purpose.
Corporate Governance	Set of principles and mechanisms whereby the organisation makes the most important decisions for its operation.
Legislative Decree 231/2001 or the Decree	Legislative Decree no. 231 of 8 June 2001, “Rules governing the administrative liability of legal persons, companies and associations, even without juridical personality”, as amended.
Legislative Decree 231/2007	Legislative Decree no. 231 of 21 November 2007 concerning the prevention of the use of the financial system for laundering revenues from illegal and terrorist financing activities, as amended by the Legislative Decree no. 90/2017 of 25 May 2017.
Employees	Individuals in an employment relationship of subordination with Fondazione Generali – The Human Safety Net ONLUS, including executives.
Executives	Individuals who, by virtue of their professional expertise, as well as hierarchical and functional powers, which are adequate to the nature of their jobs, implement their employer’s directives by organising the work activity and overseeing it.
Secondment	Mechanism whereby an employer (seconder) transfers, for its own interests, one or more workers to another party (secondee), on a temporary basis, to execute a given work assignment.

Risk Assessment Document (“RAD”)	Document prepared by an employer containing a report assessing the risks for health and safety in the workplace and the criteria for that assessment, specifying the prevention and protection measures and the personal protection equipment resulting from that assessment, the programme of measures deemed advisable to improve the levels of safety over time, identifying of the procedures for implementing the measures to be carried out, and the roles, within the organisation, assigned to that task, the name of the RSPP, of the RLS and of the occupational health physician who participated in the risk assessment, as well as a list of the assignments that may expose workers to specific risks and that require recognised professional skills, specific experience, and adequate training and coaching.
Entities	Organisations with juridical personality, companies and associations, with and without juridical personality.
Public body	<p>An entity, (i) which is incorporated, (ii) set up to meet specific needs of general interest without industrial or commercial purposes; (iii) alternatively, mostly financed by the State, public local authorities or other bodies governed by public law, or managed by the latter (including by appointing more than half of the members of its Board of Directors, management board or supervisory board).</p> <p>Public bodies include, but are not limited to:</p> <ul style="list-style-type: none"> - State administrations: Government, Parliament, Ministries, Ordinary and Accountant Judiciary, consulates and embassies, prefectures, central police stations, etc.; - Public Local Authorities: regions, provinces, municipalities; Local Health Authorities (ASL); - Institute for Accident Prevention and Safety in the Workplace (ISPESL); - Regional Agencies for Environmental Protection (ARPA); - Provincial Labour Departments (DPL); - Labour inspectorate; - Social Security agencies (INPS, INAIL); - Customs Agency; - Revenue Office; - Italian Society of Authors and Publishers (SIAE); - Law Enforcement (State Police, Carabinieri, food law enforcement (NAS), Fire Departments, Finance Police, etc.).
Generali Group or Group	Assicurazioni Generali and its subsidiaries according to article 2359, paragraphs 1 and 2, of the Italian Civil Code (hereinafter also referred to as c. c.).
Group Head Office	Assicurazioni Generali, which controls the other companies of the Generali Group through stock ownership.
Official in charge of a public service	A person who “renders a public service in any capacity”, meaning an activity governed in the same form as a public function, but without the typical powers attached to the latter (article 357 of the Penal Code (hereinafter also referred to as p. c.).

Internal

ANIA Guidelines	Guidelines for developing organisation, management and control models for the insurance sector in compliance with Legislative Decree 231/2001, as adopted by the ANIA Executive Board on 26 November 2002, as amended.
Confindustria Guidelines	Guidelines for developing organisation and management models according to Legislative Decree 231/2001 issued by Confindustria's Working Group on the administrative liability of legal persons, approved in June 2004, as amended.
Model	Organisation, management and control model pursuant to Legislative Decree 231/01
Surveillance Body or SB	Internal control body responsible for overseeing the operation of and compliance with the Model, as well as for its update.
Corporate bodies	The Board of Directors and the Board of Auditors of Fondazione Generali - The Human Safety Net ONLUS and their members.
Public Administration	This includes all government departments, including institutes and schools of all levels, educational institutions, State enterprises and government departments with autonomous legal status, the regions, provinces, municipalities, mountain communities and their consortia and associations, academic institutions, autonomous council housing institutions, the chambers of commerce, industry, handicraft and agriculture and their associations, all non-economic national, regional and local public entities, administrations, companies and entities of the National Health Service.
Partners	Contractual counterparties of Fondazione Generali - The Human Safety Net ONLUS, such as suppliers, distributors, both physical and legal persons, with whom the Foundation has any sort of collaboration governed by a contract (joint ventures, consortia, collaboration in general).
Public official	An individual who "exercises a legislative, juridical or administrative public function" (article 357 p. c.).
Offences	Offences (crimes and infractions) as specified in articles 24 ff. of Legislative Decree 231/2001.
Risk Assessment	Methodology for identifying and analysing risks.
Foundation	Fondazione Generali - The Human Safety Net ONLUS with registered offices in Trieste at Piazza Duca degli Abruzzi, 2.
Third parties	Subjects that do not belong to Fondazione Generali - The Human Safety Net ONLUS, but with whom it has relationships while conducting its activities.
Consolidated Law on Health and Safety in the Workplace	Legislative Decree no. 81 of 9 April 2008, implementing Article 1 of Law no. 123 of 3 August 2007 on health and safety in the workplace.
Top Management of the Organisation	The General Secretary as well as all the executives with strategic responsibilities, who are responsible, at various levels, for implementing, maintaining and monitoring the Internal Control System, in compliance with the instructions of the Board of Directors.

Internal

GENERAL PART

Foreword

On 8 June 2001, in execution of the delegation referred to in Law no. 300 of 29 September 2000, the Italian Parliament issued the Legislative Decree no. 231 (hereinafter referred to as the “Decree”), which contains “Rules governing the administrative liability of legal persons, companies and associations, even without juridical personality”, thus aligning the Italian regulations on corporate liability to a number of international conventions.

The entry into force of the Decree introduced the notion of administrative liability of legal persons into the Italian legal system. That liability arises from the commission of specific offences by:

- persons holding positions of representation, administration or guidance of the organisation or one of its organisational units with financial and functional autonomy, as well as persons who manage and control the organisation, including *de facto* (“individuals in senior positions” or “Senior Officials”);
- persons subject to the steering or supervision of one of the subjects described above (so-called “persons in a subordinate position” or “Subordinate Subjects”).

In order for the organisation to be liable, the Decree requires that:

- one of the “predicate offences” identified by the Decree itself be committed;
- the offence be committed in the interests or to the benefit of the Entity;

A form of exemption from administrative liability is, however, envisaged whenever the Entity has adopted and effectively implemented an “Organisation and Management Model” suitable for preventing the criminal offences identified by the Decree.

1 The Organisation and Management Model of Fondazione Generali - The Human Safety Net ONLUS

Fondazione Generali - The Human Safety Net ONLUS (hereinafter also referred to as the "Foundation") only pursues the goals of social solidarity described in article 10 of Legislative Decree no. 460 of 4 December 1997, carrying out, *inter alia*, activities in such sectors as: social and healthcare; charity, education, and training; development cooperation and international solidarity; protection of civil rights; support for scientific research of particular social interest or by assigning those activities to universities, research institutions and other foundations that carry them out directly, in areas and in ways that are consistent with the current regulatory framework.

The Foundation, thanks to the support of the Generali Group, is open to alliances and partnerships between private individuals and organisations that share its values and mission.

1.1 Governance Model of the Foundation

In view of the peculiarity of its organisational structure and of its activities, the Foundation has adopted a governance model of its own, which is based on some key principles, such as the central role played by the Board of Directors, the proper management of conflicts of interest, the transparency in the disclosure of its management decisions, and the efficiency of its System of Internal Controls.

According to its Statute, the Foundation translates those principles into the activities performed by the following main corporate bodies:

- Board of Directors
- Executive Committee
- Board of Auditors

The **Board of Directors** (hereinafter also referred to as the "administrative body") is appointed by Assicurazioni Generali S.p.A., which also determines the number and duration in office of its members and appoints Chairman of the Foundation, by choosing him/her from among the members of the Board of Directors of the Foundation.

The Board of Directors is vested with all the broadest powers for administering the Foundation and its assets, as well as any other resources connected with its purposes.

The Board of Directors can appoint an **Executive Committee** of three members, setting their responsibilities and powers. The members of the Executive Committee must sit on the Board of Directors. The Board appoints a **Secretary**, who must not necessarily be one of its members.

The **Board of Auditors** consists of three standing members and two alternate members appointed by the Board of Directors of Assicurazioni Generali. This Board confirms the operating decisions, ensures that accounting records are kept meticulously and that asset valuations are well-founded; it provides its opinion by drawing up an *ad-hoc* report on the final account of each financial year.

1.2 The System of Internal Controls

The founding elements of the system of internal controls may be represented by the combination of the following aspects, which imbue the organisation at every level:

- internal control environment
- internal control activities
- awareness
- monitoring and reporting.

The Board of Directors ensures that, at any given moment, the internal control and risk management system is in line with the current regulations, the Guidelines and Policies of the Generali Group and, to this end, conducts an assessment of its consistency with those standards, at least on an annual basis.

The Board of Directors is responsible for ensuring compliance with the laws, regulations and other applicable standards.

It is also responsible for implementing, maintaining and monitoring the internal control and risk management system.

Furthermore, for the purposes of this Model, the following qualifying elements are particularly significant:

- control system of management and of financial flows;
- accounting control system;

- computer systems;
- outsourcing contracts;
- control and behaviour safeguards according to Legislative Decree 231/2001.

1.3 Construction of the Model

In compliance with the provisions of the Decree, the Foundation adopted its own Organisation Model through a resolution of its Board of Directors. Both the adoption and any subsequent modification of this document are the exclusive responsibility of the administrative body.

In order to formulate the Model, reference has also been made to the Guidelines issued by the Italian association of insurance companies (ANIA) and to those issued by Confindustria (the Italian Manufacturers' Association), to the best practices regarding the administrative liability of organisations (corporate criminal liability), to the main legal doctrine and case law and to the outcomes of the Risk Self-Assessment activities that have been conducted. The Model has been developed considering the structure and the activities materially performed by the Foundation, the market and the nature and size of its organisation. The Foundation carried out a preliminary analysis of its business environment, then an analysis of the activities with potential risk profiles in connection with the offences specified in the Decree. In particular, the following aspects were studied: the history of the Foundation, the reference context, the sector to which it belongs, the organisational chart, the existing corporate governance system, the system of proxies and delegations, the existing juridical relationships with third parties, the operational situation, the practices and procedures that have been formalised and disseminated within the Foundation for the performance of its operations.

This version of the Model has been developed following an approach favouring simplicity and compatibility with the existing control system, in order to be as comprehensible and as easy to read as possible for the addressees, also ensuring a high level of customisation to the specific operations of the Foundation.

In order to develop this Model, the following measures were taken:

- the sensitive activities in which the predicate offences specified in the Decree may be committed were identified. To this end, the Heads of the corporate functions have been interviewed, and the internal organisational charts, the responsibilities allocation system (the so-called Roles & Mandates), and the internal processes and procedures regarding sensitive activities were analysed;
- the various risk owners assessed the risks of offences being committed (through so-called Risk Self-Assessments);
- the control safeguards needed to prevent the crimes specified in the Decree and applying to the Foundation were identified and assessed.

The internal working group has developed a Risk Self-Assessment matrix aimed at updating the mapping of sensitive and/or instrumental activities with respect to each corporate process considered critical in accordance with 231 Decree. The matrix consists of various sections, which can be summarised as follow:

- 1) sensitive/instrumental activities connected with the reference value chain processes;
- 2) functions managing the sensitive/instrumental activities under analysis and reference to possible outsourcers;
- 3) specification of the categories of predicate offences, including examples of possible offences and of the potential relevant unlawful behaviours for each sensitive activity;
- 4) evaluation of the inherent risk divided by its probability of occurrence and its potential impact;
- 5) main control safeguards that can mitigate the inherent risk, evaluation of the internal control system and assessment of the residual risk.

The Model is one of the internal regulations of and is binding for the Foundation.

Finally, please note that the Addressees of the Model are required to abide by the rules contained therein, even when the sensitive activities – as identified in the special part – are carried out by and/or outsourced to other companies of the Generali Group by virtue of specific contractual causes included in outsourcing contracts.

1.4 Structure of the Model

The Organisation Management and Control Model under Legislative Decree 231/2001 (hereinafter referred to as the "Model") consists of a General Part, of a Special Part – which is divided into various sections -- and of annexes considered an integral part of the Model.

In compliance with the Decree, there also exists an appropriate regulatory system designed to punish any violation of the measures indicated in the Model (see Chapter 4).

General Part

The General Part, in addition to explaining the rationale and the principles of the Decree, the Governance Model, and the principles of the System of Internal Controls of the Foundation, outlines the building blocks of the Model, including the role of the Surveillance Body of the Foundation (hereinafter also referred to as "SB"), which supervises its operation, compliance and update.

The Model is also complemented by the following components of the internal control system, which contribute to strengthening the widest control system under the Decree.

- Code of Conduct (see chapter II, paragraph 1);
- Organisational system (see chapter II, paragraph 2);
- System of powers (see chapter II, paragraph 5);
- Internal Regulatory System (see chapter II, paragraph 6);
- Management and financial flow control system (see chapter V, paragraph 7);
- Control safeguards under Legislative Decree 231/01 (see chapter II, paragraph 8);
- Preparation and dissemination plan for the Model (see chapter II, paragraph 9).

Special Part

The Special Part is divided into several sections for each category of offences which is considered relevant for the Foundation. The offences, as referred to in the Decree and potentially relevant for the Foundation, were identified based on a Risk Self-Assessment, also considering the sector of operation, the corporate structure and the processes characterising the Foundation.

To this end, each section of the Special Part contains:

- the analysis of each offence contained in the Decree from a regulatory viewpoint;
- the list of sensitive activities which may potentially give rise to the offences described in this section, as well as some examples of ways in which they can be committed;
- the general principles of conduct by which the Addressees of the Model shall be guided;
- the specific control principles (so-called "preventive controls") associated with the corporate functions involved in each of the sensitive activities and any other applicable control safeguards contributing to preventing the offences identified.

In detail, the sections of the Special Part are as follows:

- Section **A**, regarding offences against the Public Administration (articles 24 and 25 of the Decree) and private-to-private corruption (article 25-ter of the Decree);
- Section **B**, regarding computer crimes (article 24-bis of the Decree);
- Section **C**, regarding organised crime offences (art. 24-ter of the Decree) and transnational crimes (article 10 of Law no. 146 of 16 March 2006);
- Section **D**, regarding crimes of counterfeiting in currency, legal tender, revenue stamps, and distinctive signs (article 25-bis of the Decree);
- Section **E**, regarding corporate offences (article 25-ter of the Decree);
- Section **F**, regarding crimes of manslaughter and serious or very serious injuries committed in violation of the laws on the protection of health and safety in the workplace (article 25-septies of the Decree);
- Section **G**, regarding crimes such as handling stolen goods, money-laundering and using money, goods or assets of unlawful origin, as well as self-laundering (article 25-octies of the Decree) and crimes of terrorism or subversion of the democratic order (article 25-quater of the Decree);
- Section **H**, regarding offences related to copyright violations (article 25-novies of the Decree);
- Section **I**, regarding crimes of instigation not to testify or to give false testimony before court authorities (article 25-decies of the Decree);
- Section **J**, regarding environmental crimes (article 25-undecies of the Decree);
- Section **K**, regarding the employment of foreign nationals with irregular residence permits (art. 25-duodecies of the Decree), as well as crimes against the individual, including the crimes referred to in article 603-bis p. c.: "Illicit brokering and labour exploitation" (art. 25-quinquies of the Decree).

As concerns the single offences listed above, the general control principles are applied, which are described in the General Part, as well as the general conduct principles and preventive control principles described in the Special Part.

With regard to crimes against industry and trade (article 25-bis.1 of the Decree), market abuse (article 25-sexies of the Decree), and female genital mutilation practices (article 25-quater 1), considering the core business of the Foundation, the social-economic environment in which it operates and its usual legal and economic relationships with third parties, there are no reasons to believe the Foundation could face the risk of these crimes being committed in its interests or for its benefit. In this respect, the related risks were however safeguarded by including suitable behavioural principles in the Code of Conduct binding, however, the addressees to respect core values such as solidarity, respect for human life, morality,

Internal

fairness and legality.

1.5 Addressees of the Model

The addressees of the Model (hereinafter referred to as “Addressees”), who commit themselves to comply with it, are:

- those who perform – including *de facto* – functions of representation, management, administration, steering or control of the Foundation or of one of its organisational units, which is financially and functionally independent;
- employees and contractors of the Foundation, at any level and with any type of contractual relationship, including those seconded abroad or at companies of the Generali Group;

The Addressees are required to fully comply with all the provisions of the Model (General Part and Special Part) and of the Code of Conduct, while also fulfilling the duties of fairness and diligence arising from their legal relationships with the Foundation.

Furthermore, the basic principles of the Model or some of its parts, for relevant aspects, bind , by virtue of specific contract clauses, all Third Parties which, albeit not part of the Foundation, operate on its behalf or in its interests.

2 Components of the Organisation and Management Model

2.1 Code of Conduct

The Code of Conduct sets the main conduct rules which all employees, the administrative body of the Foundation, and third parties interacting with it are required to observe in their behaviours.

In particular, the Code of Conduct governs the relationships with colleagues, customers, competitors, suppliers and with other stakeholders: it defines rules for social fairness and social liability in the conduct of business, the protection of the working environment and the promotion of diversity and inclusion, the protection of corporate assets, the monitoring of conflicts of interest, the fight against corruption, the management of relationships with competitors, the selection of suppliers, financial information, the prevention of money-laundering and terrorist financing.

The Code of Conduct is complemented by a system of Implementing Provisions, which, since they represent a set of minimal, unavoidable standards of behaviour, can be expanded or specified by adopting further regulations.

In particular, the following Implementing Provisions are referred to:

- promotion of diversity and inclusion
- conflicts of interest
- fight against corruption
- management of participations in institutional events
- personal data and privacy.

The prescriptions of the Code of Conduct and of the respective Implementing Provisions complement the Model and any violations thereof may be punished by applying the penalties described in this General Part of the Foundation's Model.

All addressees of the Code of Conduct are responsible for being aware of and complying with it and with the relevant Implementing Provisions, as well as with the other relevant internal rules according to their tasks.

Any third parties acting on behalf of the Foundation (consultants, suppliers, etc.) must also adhere to the principles of the Code of Conduct.

Although the Model and the Code of Conduct have different functions, they are prepared according to common principles and rules with a view to achieving a consistent and efficient set of internal rules.

2.2 Organisational System

The organisational system of the Foundation is characterised by an accurate definition of the responsibilities and tasks of each operating area, of hierarchical lines of reporting and their responsibilities.

The documentation that the Foundation uses to represent its organisational system and to regulate its actions, including in connection with sensitive activities under its Organisation and Management Model, includes the following:

- organisational charts
- documents describing key roles and responsibilities (Roles & Mandates, service orders and other documents).

For an overview of the Foundation's organisational system, refer to the information published on the intranet or web site.

2.3 Remuneration and incentive scheme

An important component of the organisational system of the Foundation is the remuneration and incentive system for all its employees and for those who, although not employees, act within its mandate or in its interests.

The Foundation's system of remuneration and incentives is designed, first of all, to remunerate their roles, in view of the responsibilities assigned, and the skills and capabilities shown by them. Secondly, the system aims to reward the results obtained, in line with the behaviours shown to achieve them, which must reflect constant compliance with the applicable laws and regulations, with the Code of Conduct, with the Model and with the existing procedures, with a view to accurately assessing risks, and to appropriately readjusting the relevant actions on a wider time span, so as to achieve results more easily, both in the short and in the medium-long term.

In other words, the Foundation adopted a system that sets reasonable goals, and also emphasises the quality and behavioural element in the employees' performances, while being designed to reward not just quantitative results but also the ability to express organisational skills through behaviours that are consistent with the values enshrined in the Code of Conduct.

These principles also apply to individuals who work by mandate or in the interests of the Foundation.

2.4 Outsourced processes

In order to achieve the objectives indicated in its Statute, the Foundation collaborates with resources seconded by Assicurazioni Generali S.p.A. and may collaborate with the structures of the Parent Company or of other Group companies, in accordance with their procedures.

In support of its operations, the Foundation enters into outsourcing agreements both with Generali Group companies, and with external counterparties, but, should outsourcing practices be resorted to, they do not exempt in any way the bodies and senior management of the Foundation from their responsibilities.

For this purpose, the Foundation has set up an internal system that confers powers by assigning specific delegations and proxies consistent with the organisational responsibilities in question.

2.5 System of powers

The Internal Control System of the Foundation is also based on a formalised structure of powers, which is an integral and substantial part of this Model and, as such, is appropriately disseminated within the Foundation.

The Chairman of the Foundation is vested with specific powers and authorities which are instrumental in exercising the proxies granted him/her by the Board of Directors itself. Within the delegated powers, the Chairman may sub-delegate to employees or even to third parties one or more powers and responsibilities that have been granted to him/herself, within any limits to be set in advance. The individual executives may in turn delegate their subordinates (executives and officials).

2.6 Internal Regulatory system

As stated above, the Foundation avails itself of resources seconded from Assicurazioni Generali or from other Group companies and of the collaboration of structures of those companies. In this context, it should be emphasised that the companies of the Generali Group, by issuing the GIRS Policy, adopted the “Generali Internal Regulations System” (GIRS) framework. That regulatory framework is aimed at defining and governing the internal regulatory system, also identifying the roles and responsibilities of those involved (drawing up, updating, validating, approving, communicating, implementing and monitoring).

As a consequence, the above-said seconded resources work in compliance with the internal regulatory system described above.

The following is the regulatory hierarchy making up the GIRS framework:

- Group Policy
- Group Guideline
- Technical Measures

The Group Policies – which are subject to the approval of the Board of Directors of the Foundation and, as a rule, are binding for all Group companies - contain high-level principles aimed to achieving fundamental goals for the Group and/or at issuing provisions connected with the Internal Control and Risk Management System. The Group Policies, following their approval by Assicurazioni Generali, are submitted by the senior executives of the other Group companies to the competent administrative, governing and supervisory bodies for approval, taking into account any necessary waivers justified by any conflicts with local regulations.

The Group Guidelines – which are subject to the approval of the Foundation’s Group CEO and, as a rule, are binding for all Group companies – seek to regulate issues concerning one or more corporate functions. The Group Guidelines, following their approval by Assicurazioni Generali, are subject to the approval of the executives of the other Group companies, taking into account any necessary waivers justified by any conflicts with local regulations or by criteria of proportionality connected with specific Group companies.

The Technical Measures aim to provide operational provisions with an inter-departmental impact, including those that further regulate the matters introduced by a Group Policy or Guideline. They must be approved by the Head of the Functions owning the regulated process, in line with the corresponding reporting system and with the system of powers of Assicurazioni Generali.

Overall, therefore, the internal regulatory system adopted by the Foundation also aims to govern the management of sensitive activities, in line with the Model’s provisions, since it represents the body of rules to be followed while conducting corporate activities.

2.7 Management control and control of financial flows

Financial flows are managed in compliance with the principles of traceability of transactions and of consistency with the

assigned powers and responsibilities.

The management control system of the Foundation includes mechanisms for checking the management of resources that must ensure, in addition to the verifiability and traceability of expenses, the efficiency and cost-effectiveness of the Foundation's activities. More specifically:

- the resources – both financial and non-financial – available to the individual functions and organisational units and the scope within which those resources may be employed, by programming and setting the budget, are defined clearly and systematically;
- any deviations from planning assumptions are detected, their causes are analysed, and the results of the assessments are reported to the appropriate hierarchical levels for the required adjustments by preparing the final balance statements;
- continuous monitoring helps detect any process anomalies, then the necessary in-depth analyses and any corrective actions are performed.

In order to achieve these goals, the planning process, as duly formalised, ensures:

- the collaboration of a number of authorised individuals to the determination of the available resources and areas of expenditure, with the goal of ensuring constant cross checks and audits for a given process/activity, as well as adequate segregation of the functions and continuous monitoring of any deviations;
- the adoption of appropriate and homogeneous procedures for the economic evaluation of initiatives so as to compare the economic values of various organisational units;
- the adoption of plans to identify the best corrective strategy.

The activities connected with management control ensure constant verification of the consistency of the goals achieved with the actual expenses incurred and with the commitments undertaken in the planning phase.

If the analyses and/or the requests for authorisation show major deviations from the budget which are not justified, and if the information is to be considered significant, also with reference to the contents of the Decree, the organisational unit responsible for management controls is required to inform the Surveillance Body.

For further details on the management of financial resources and on the budget, please refer to the specific Sections of the Special Part.

2.8 Control safeguards as per Legislative Decree 231/2001

The system of preventive controls put in place by the Generali Group – and applied by the Foundation – is implemented so as to be only circumvented intentionally, also to exclude the organisation's administrative liability.

That said, this paragraph illustrates the criteria for selecting the control safeguards preventing the risk that the crimes specified in the Decree be committed. There are **three levels** of safeguards:

- **General control principles** by which, regardless of the degree of significance of the individual types of crime or of the level of risk underlying each sensitive activity identified, the Foundation is guided in the design of its system of controls:
 - **Segregation of activities:** between those who execute, those who control, and those who authorise any operations¹;
 - **Formal rules:** i.e. company directives providing at least general reference principles for the regulation of activities, responsibilities and controls;
 - **Delegations and proxies:** formal rules should be envisaged for exercising delegations and proxies, as stated in paragraph 5 of this chapter;
 - **Traceability:** the individuals, functions/organisational units concerned and/or the information systems used must ensure the identification of the sources, informative elements, and controls that support decision-making processes and the procedures for managing the financial resources of the Foundation;
 - **Archiving/keeping documents:** the documents on the Foundation's activities must always be stored and kept by the responsible structures, to prevent any subsequent changes, without specific evidence, and to allow access only to the relevant authorities, according to internal rules, and to supervisory bodies.
 - **Confidentiality:** access to any documents already stored, as mentioned in the previous item, is granted to the head of the function and to any delegates thereof. Such access is also granted to the relevant bodies and supervisory functions, such as the members of the Board of Auditors, of the Surveillance Body, etc.
- **General principles of conduct**, which include special provisions regulating the procedures for making and implementing decisions, within each category of offences held as relevant;
- **Specific control principles**, which consist in control safeguards aimed at preventing crimes from being committed in

¹The principle is the following: the segregation consists in codified, complex and structured systems where the distinct stages are identified and regulated, in their management – with limited discretionary power in their implementation – and can be tracked in the decisions.

each of the “sensitive activities” which are mapped and specified in the sections of the Special Part of this Model.

A further level of control is offered by specific Guidelines which are drawn up and issued for the purposes of Legislative Decree 231 and included in the internal regulatory system.

In addition to those Guidelines, all the Policies and Operating Procedures issued according to the GIRS System and referred to in the Model, are an integral part thereof.

Any failure to comply with the instructions of those regulations, as mentioned in the Model, could be punished according to the instructions of Chapter 4 (Penalty System).

2.9 Plan for Disseminating the Model and for the relevant Training of Staff

In order to effectively implement its Model, the Foundation ensures that its contents and principles are disseminated inside and outside it.

In particular, the Foundation’s goal is to extend the dissemination of the contents and principles of the Model not only to its employees but also to individuals who, although not formally employed, work, including occasionally, to achieve the Foundation’s objectives by virtue of contracts, and who can be led or supervised by the Foundation.

The Model is formally provided:

- to the Directors, to the Secretary General and to the Board of Auditors, by publishing it on the corporate intranet or by forwarding electronic copies thereof;
- to the Foundation’s staff through by publishing it on the intranet;
- to third parties according to methods defined from time to time according to the kind of counterparty in question.

In particular, it is the Surveillance Body’s responsibility to promote the dissemination of the Model and to monitor all the information activities for the Addressees, also by promoting specific initiatives and information plans aimed at fostering adequate knowledge and awareness of the Model and of the related procedures.

In addition to the activities aimed at informing the Addressees, the Foundation’s SB is required to organise their regular training and to advance and monitor the implementation of initiatives favouring it; that body may request periodic checks on the Employees’ level of knowledge of the Model.

The principles of the Model, in particular those of the Code of Conduct within it, should be illustrated to the Foundation’s resources through specific training activities², whose attendance should be mandatory, and whose implementation is submitted for approval to the SB through specific plans drawn up and implemented by the Foundation.

Furthermore, in order to facilitate the understanding of the Model, the Foundation organises – through the organisational unit responsible for trainings – different training paths based on the analysis of skills and training needs, and devoted to specific categories of addressees: employees in general, employees who perform specific sensitive activities, the Surveillance Body, the directors, etc. The training activities can be provided through e-learning courses and/or in the classroom. To round off the training activities, questionnaires checking the level of learning need to be filled in. Classroom training is conducted by experts on the contents of the Decree.

Training for the implementation of the Model is mandatory for all the recipients identified in chapter 1, paragraph 5 Addressees of the Model.

3 Surveillance Body

3.1 The Surveillance Body of Fondazione Generali – The Human Safety Net ONLUS

Appointment and composition

In compliance with article 6, paragraph 1 b) of the Decree, the Foundation identifies the Surveillance Body as a single-member body, who is appointed through a Board of Directors resolution, consisting in an authoritative and competent external professional with a proven track record on subjects related to the tasks assigned to the SB.

The above composition is considered suitable by the Foundation because it meets the following requirements:

- autonomy and independence, since:
 - the activities performed by the SB are not subject to any interference whatsoever and/or to conditioning by any parties within the Foundation and, therefore, the single member of the SB cannot in any way be subjected either to negative consequences of any nature or to any disciplinary sanctions for his/her decisions and

² For instance, through courses, seminars, etc.

- opinions expressed in good faith;
 - the impartiality principle is guaranteed, the SB is appropriately placed, as it reports directly to the Board of Directors;
 - he/she is not entrusted with any tasks which are directly or indirectly linked to the Foundation's decision-making and their implementation;
 - the SB has enough financial resources at its disposal to properly conduct its activities;
- professionalism, since:
 - the external professional, i.e. the single member of the SB, was selected for his/her specific professional skills in the legal, economic and financial fields.
- good repute and absence of conflicts of interest, since the absence of causes for ineligibility and/or incompatibility of the single member of the SB has been determined and is monitored over time.

The SB is appointed by the Foundation's Board of Directors, which must first evaluate and certify:

- the requirements of independence, autonomy, and continuity of action that should characterise the Body's actions;
- the subjective requirements for the member's eligibility.

The single member of the SB is formally designated by a specific letter of appointment that also stipulates his/her remuneration.

The SB acts independently from the Board of Directors and from the others surveillance bodies of Generali Group companies (including parent companies and/or principal companies for outsourced services), with which it promotes forms of cooperation and takes part in meetings, within the limits listed in the following paragraphs, and on equal footing, excluding any interference in their respective responsibilities and activities.

Term in office and causes of termination

The term in office for the SB member is three years and is renewable, with a limit of three mandates.

When the term expires, and pending a new appointment, the SB's sole member must serve for three additional months, at the end of those three months, the Board of Directors must appoint a new SB without delay.

The SB may be removed from office for one of the following causes:

- expired term of office;
- withdrawal of its single member, by a formal written notice sent to the Board of Directors;
- revocation of the SB by the Board of Directors.

In order to ensure that the SB is absolutely independent, it can only be removed for just cause, namely one of the following:

- serious negligence in the performance of his/her duties, including violation of confidentiality obligations;
- due to one of the causes of expiry and/or incompatibility specified in the following paragraph "Subjective requirements for the eligibility of the member of the Surveillance Body";
- any involvement of the Foundation in a criminal or civil proceeding related to omitted or inadequate supervisory activity, including with negligence;
- in general, the removal for just cause is ordered by resolution of the Board of Directors, after hearing the Board of Auditors.

Further reasons for the SB's removal are:

- serving as director in one of the companies of the Group;
- unjustified absences from two consecutive meetings of the Body within a corporate year;
- assigning functions and operational responsibilities within the Foundation's organisation which are incompatible with the requirements of autonomy, independence and continuity of action of the SB.

In the event of expiry, removal or withdrawal, the Board of Directors promptly appoints a new SB.

Subjective requirements for the eligibility of the single member of the Surveillance Body

The reasons for the ineligibility and/or incompatibility of the SB member are as follows:

- being or becoming a non-independent member of the Board of Directors;
- existence of relations of consanguinity, marriage or kinship down to the fourth degree with members of the Board of Directors or of the Board of Auditors of the Foundation;
- engaging in direct or indirect economic relationships, excluding permanent employment, economic and/or contractual

relationships, with or without remuneration, with the Foundation of such significance as may undermine their independence;

- having of conflicts of interest, even potential ones, with the Foundation, after stating them specifically upon his/her appointment;
- having performed, at least in the three years prior to his/her designation, administrative, management or control functions in companies under bankruptcy, administrative compulsory liquidation or equivalent procedures or in companies operating in the credit, financial, securities or insurance sectors under extraordinary administration;
- having been indicted for one of the predicate offences mentioned in the Decree or, however, of the same nature;
- having been sentenced, including with a non-irrevocable sentence, for other offences than those described in the Decree, except for rehabilitation purposes or in the event of extinguishment of the offence;
- being legally incapacitated, under care, bankrupt or sentenced to a punishment involving a disqualification, even temporary, from holding public offices or being incapacitated to hold management offices.
- being temporarily disqualified or suspended from holding management offices in corporations and enterprises;
- being in one of the conditions for ineligibility or withdrawal laid down in article 2382 c. c.;
- having been subjected to preventive measures according to Law no. 1423 of 27 December 1956 or Law no. 575 of 31 May 1965, as amended, with the exception of rehabilitation;
- in the event of conviction or plea-bargain, even without a final judgement, or with the sentence conditionally suspended. The exceptions, due to the rehabilitation or resolution of the offence, are listed below:
 - for one of the offences set forth in Royal Decree no. 267 of 16 March 1942 (law on bankruptcy);
 - for one of the offences provided for in Title XI of Book V of the Civil Code (companies and consortia);
 - for a crime against the Public Administration, against the public trust, against property, against public economy, or for a tax crime;
 - for one of the crimes envisaged by the norms applicable to the following sectors: banking, finance, insurance, securities market and payment tools;
 - for any other offence committed with criminal intent, for a period not less than one year.

Should, during the term of office, a cause for expiry arise, the single member of the SB is required to immediately inform the Board of Directors.

The resources of the Surveillance Body

Every year the Board of Directors, on the SB's proposal, resolves on the allocation of the financial resources necessary to perform the duties assigned to it (budget).

The SB may ask the Chairman of the Board of Directors, by means of a written reasoned statement, to allocate additional resources, when the need arises in the course of its activities.

The Surveillance Body, while performing its assigned duties, collaborates predominantly with Group Audit and Group Compliance functions of Assicurazioni Generali S.p.A, availing itself of their expertise and professionalism while conducting surveillance activities. By doing so, the SB guarantees a high level of professionalism and continuity of action.

The SB also avails itself of the Group's "Legislative Decree 231/01" unit, which offers its support to updating the Model and to overseeing the implementation of the Organisational Model, to managing the technical secretariat of the Body, facilitating the coordination between the various corporate functions and the SB itself, defining the annual training plan and monitoring periodic flows.

The SB may also seek the collaboration of other organisational units of the Foundation or of the Group for supervisory activities requiring specific professional expertise.

While performing the activities requested by the SB, all the human resources involved, although continuing to report to their hierarchical superiors, will depend functionally on the SB and will report to it for the activities assigned to them.

In addition to the resources above, the SB, under its direct oversight and responsibility, may avail itself of external consultants and professionals whose remuneration will be paid from the budget appropriation.

3.2 Duties and powers of the Surveillance Body

In the pursuit of the objectives set forth in the Decree, the following tasks have been assigned to the Surveillance Body:

- overseeing operation of and compliance with the Model;
- verifying that the Model is actually suitable for preventing the crimes specified in the Decree from being committed;
- analysing whether the adequacy and functionality required of the Model persist over time;
- promoting constant updating of the Model and to the system overseeing its implementation, in collaboration with the organisational units concerned, suggesting to the Board of Directors any corrections and adjustments, where required;

Internal

- entertaining relationships with and ensure information flows to the Board of Directors and the Board of Auditors;
- provide information to the Board of Directors and to the Board of Auditors on issues of common concern, also through formal hearings, if so required;
- ensuring that the individuals concerned duly perform all the reporting activities prescribed by the Model;
- promoting constant updates to the system for identifying, mapping and classifying the sensitive activities for the SB's own supervisory role;
- developing a surveillance plan which is consistent with the principles enshrined in the Model, within the various sensitive activities identified;
- ensuring the implementation of the surveillance plan, also by scheduling the activities and by conducting unplanned, non-programmable interventions;
- ensuring the preparation of reports on the results of the interventions made;
- where considered appropriate and with reference to processes wholly or partially outsourced to Generali Group companies, encourage the examination of the whole sensitive process:
 - communicating in advance to the outsourcer's SB the verification activities to be carried out to reach some common planning for surveillance activities;
 - acquiring the outcome of the verification activities conducted by the outsourcer's surveillance body;
- without prejudice to the provisions of paragraph 9 of chapter 2, defining and promoting initiatives aimed at disseminating the knowledge and understanding of the Model, as well as training the staff and raising their awareness about the compliance with the principles contained therein, also with the support of the specific structures in the Foundation and in the companies of the Generali Group;
- providing clarification on the significance and application of the provisions contained in the Model, also with the support of the competent functions of the Foundation and of the companies of the Generali Group;
- ensuring effective implementation of the internal communication system to allow reports to be transmitted and collected for the purposes of the Decree, while ensuring that the authors of those reports are protected, and their identity remains confidential;
- examining and evaluating the information and/or reports received and related to compliance with the Model, including information about any violations;
- verifying and assessing the fitness of the disciplinary and penalty system;
- making sure that, after the inquiries, any disciplinary measures against any individuals who violated the Model are considered and that the most appropriate penalty for the case at hand is proposed;
- providing the necessary information support to the inspection bodies or to the authorities that require them.

In order to fulfil its duties, the SB is vested with all the powers needed to oversee accurately and effectively the operation of and compliance with the Model.

While performing its delegated duties, the SB may without prior notice or authorisation, for example:

- conduct audits and inspections to ascertain any violations of the Model, or those which are deemed advisable for properly performing its duties;
- monitor the Organisation's conduct, also via random checks of documents and operating processes;
- hear the staff, when necessary, so that they can provide useful indications or information about the Foundation's activity or about any shortcomings or breaches of the Model;
- acquire information and access documentation of any type to and from any level and sector of the Foundation and request that any employee, Director or Auditor of the Foundation promptly provide the required information, data or news to identify aspects of the various corporate activities that may be significant for the Model and to verify its actual implementation by the organisational structures;
- have access to the financial resources needed to accurately perform its duties.

In compliance with the Confindustria Guidelines, the several Bodies of the entities of the Generali Group, in full compliance with their autonomy and independence can start some forms of collaboration connected with the following aspects:

- processes encompassing multiple Group units, i.e. intragroup outsourcing;
- specific requirements of surveillance activities;
- opinion sharing at the annual meeting.

In the case of activities outsourced within the Group, the entities' SBs may activate some forms of cooperation to increase the efficacy of the surveillance activities of each SB on transversal processes or activities.

Specifically, the SBs of the principal companies can inform the SBs of the outsourcing companies of the Group about the need to intervene on potential processes/activities partially managed by the outsourcer company. The outsourcer companies' SBs autonomously evaluate the possibility to answer to these requests, by carrying out specific checks on the process phases directly managed by them.

The collected information at the end of the previously mentioned verifications can be transmitted, in compliance with

confidentiality principles, to the SBs of the principal companies.

In addition to what was previously mentioned, each Body of Group companies can, under certain circumstances, call on another SB of other Group companies to conduct activities, within their remit, which are important for the requesting Body and be informed at the end or when important events occur.

Finally, in order to ensure efficient coordination between the SBs of the Generali Group and of the Foundation, an at least annual meeting has been organised, which allows sharing:

- the “macro-themes” of common interest regarding the formulation of Organisational Models (e.g. how to carry out risk assessments, definition of common operational approaches, sharing of best practices, definition of training conditions and plans);
- the update of the models, considering legislative and jurisprudence updates;
- methods for conducting verification activities;
- the general issues emerging from surveillance activities, which suggested strengthening the safeguards of sensitive activities of common interest.

Information flows to and from the Surveillance Body

The SB must be promptly informed by all officials of the Foundation, as well as by third parties required to comply with the Model, about any news that may be relevant to its surveillance over the effectiveness, efficiency and update of the Model, including any information regarding the existence of possible violations thereof.

The SB is required to report periodically on the effectiveness, actual implementation and update of the Model to the Board of Directors and to the Board of Auditors.

The information flows to the Surveillance Body are regulated through the 231 Guideline on “Management of information flows to the Surveillance Body”, which summarises all the information flows to the SB, while also describing their transmission methods.

The information flows to the SB consist of:

- information flows defined by the Model, as divided into:
 - information flows following an event;
 - periodic information flows;
- information flows upon request by the Surveillance Body or, in other words, any information specifically requested by the SB, because it is considered relevant for overseeing the efficacy, functionality and update of the Foundation’s Model.

Reporting System

The following general prescriptions apply to the internal communication system for all the information described above.

The addressees wishing to report a suspected violation of the Organisation and Management Model or of the Group’s Code of Conduct adopted by the Foundation have a dedicated channel available which allows reports to be sent to the Surveillance Body. That channel can be accessed via:

- e-mail: OdV231@Thehumansafetynet.org;
- registered mail: Trieste (TS), Piazza Duca degli Abruzzi, 2, Attention of the Surveillance Body.

The Company, in view of the rules introduced by Law 179/2017 “Provisions for the protection of individuals who report crimes or irregularities of which they have gained knowledge within a public or private work relationship (so-called whistleblowing)”, also set up an additional channel for reporting the aforementioned violations, which ensures that the whistle-blower’s identity remains confidential.

Any reports of suspected violations of the Organisation and Management Model or of the Code of Conduct of the Company received through the channels described above must be promptly forwarded to the Supervisory Body, so as to appropriately assess them, with the operational support of internal structures of the Generali Group companies.

The Surveillance Body is required to evaluate the reports received, giving rise, where necessary, to the necessary investigations in connection with the phenomena represented and to assess the truth and relevance of the contents of the report.

Internal

The Company undertakes to take suitable measures, including disciplinary sanctions, to guarantee the confidentiality of the identity of the whistle-blower in the various reporting stages.

The Company also undertakes to protect the whistle-blower from any application - for reasons connected to his/her reports - of discriminatory or retaliatory measures (e.g. sanctions, demotion, dismissal, transfer or other organisational measures that may have a negative effect on working conditions).

Reporting by the Surveillance Body

The Surveillance Body must conduct adequate reporting activities, either periodic or *ad-hoc*, to the Board of Directors or to the Board of Auditors.

With particular regard to periodic information flows, the Surveillance Body is required to:

- draw up, at least quarterly, a written report to the Board of Directors on any reports received, any proposals for adjustments or updates of the Model, any confirmed violations of the Model and proposed sanctions, the verification plan for the following corporate year and the state of implementation of the Model, with reference to the outcomes of the verification activity;
- meet, at least once a year, with the Board of Auditors to discuss issues of interest to both bodies;
- meet, whenever required by the involved bodies, the Board of Auditors to discuss specific topics regarding the compliance with the Model.

Finally, the single-member SB meets, at least annually, with the Chairman of the Board of Directors to inform it about significant topics related its activities.

The Surveillance Body, by implementing and activating *ad-hoc* information flows, which are distinct from periodic information flows, is required to immediately submit a memorandum to the Board of Directors about any extraordinary situations or requiring urgent intervention (e.g. violations of significant aspects of the Model) or to ask to be heard by the Board of Directors or by the Board of Auditors.

Any information and reports envisaged by the Model, is stored by the SB in a specific limited-access hardcopy and/or electronic archive.

4 Penalty System

4.1 Functions of the Disciplinary and Penalty System

Article 6, paragraph 2 e) and article 7, paragraph 4 b) of the Decree require, as a condition for effectively implementing the Organisation, Management and Control Model, for a disciplinary system to be introduced, which will sanction any breaches of the measures indicated in the Model. Therefore, the creation of an effective disciplinary system is an essential prerequisite for the mitigating value of the Model for the administrative liability of entities.

The sanctions envisaged in the disciplinary system will be applied to any violation of the Model's provisions, regardless of the course or outcome of the criminal proceeding that the court authority may have initiated as long as the conduct to be reprimanded corresponds to a type of crime relevant to the Decree.

The penalty system must be based on the principle of proportionality between the violation and its sanction.

4.2 Disciplinary offences and sanctions

Measures against employees

The Foundation's employees must comply with the provisions and rules of conduct set forth in the Model and of the obligations pursuant to article 2104, paragraph 2 c. c., the content of the Model being a substantive and integral part of those obligations.

Any violation of the individual provisions and rules of conduct of the Model, as specified in the "Disciplinary Rules" by Foundation employees, who are subject to the National Collective Contract, which governs the relationships between insurance companies and non-executive employees, is always a disciplinary offence.

The Foundation's relevant internal regulations, also mentioned in the Model, whose non-compliance is to be punished, are made available to all employees through the dissemination and training tools described in chapter 2, paragraph 9, and are binding for all the Foundation's employees.

Each report of a violation of the Model made by the Surveillance Body triggers an investigation designed to determine any

liability for the violation.

In particular, according to applicable regulations, at the investigation stage, the employee is previously charged with the offence and is also given sufficient time to present his/her defence and justification. Once the liability has been confirmed, a disciplinary sanction that is proportional to the seriousness of the violation is imposed on the offender.

The sanctions that can be imposed on Foundation employees, pursuant to article 7 of Law 300 of 30 May 1970 (the so-called "Workers' Statute") and any applicable special laws, are those prescribed by law as well as by the sanction mechanism of Employment Contracts, more specifically:

- verbal reprimand. It occurs when the workers who violate one of the internal procedures set forth in the Model³, or who, while performing sensitive activities, engage in a conduct that is not compliant with the Model's requirements. That conduct corresponds to failure to comply with the Foundation's instructions;
- written reprimand. It occurs when workers repeatedly violate the procedures set forth in the Model, or, while performing sensitive activities, engage in a conduct that is not compliant with the Model's requirements. Such conduct constitutes a repeated failure to comply with the instructions issued by the Foundation;
- suspension from service and from remuneration for a period not exceeding ten days. This measure is applied to workers who, while violating the internal procedures set forth in the Model, or by adopting, while carrying out sensitive activities, a conduct which does not comply with the prescriptions of the Model, cause damages or create situations of potential hazard for the Foundation, or to workers who repeatedly violate the procedures set forth in the Model or who, within sensitive activities, engage in a conduct that does not comply with the Model's prescriptions. Those behaviours, which result from their failure to comply with the instructions issued by the Foundation, cause damage, albeit potential, to the assets of the Foundation and/or are actions against the interests of the Foundation and/or expose it to potential administrative or interdictory penalties;
- termination of employment for justified subjective reasons. It occurs when workers who, while performing sensitive activities, engage in conducts that do not comply with the Model's requirements and constitute a significant breach thereof, aimed unequivocally at perpetrating a crime punished by the Decree or that determine the actual application of the relevant measures against the Foundation. Those behaviours represent cases of significant non-observance of the instructions issued by the Foundation and/or serious violations of the workers' obligation to co-operate for the prosperity of the Foundation;
- termination of employment for just cause. It occurs when workers who, while conducting their sensitive activities, engage in behaviours that do not comply with the Model's prescriptions and constitute significant breaches thereof, which are unequivocally aimed at committing a crime sanctioned by the Decree or that determine the actual application of the Decree's measures against the Foundation, or workers who repeatedly violated the internal procedures of the Model or who, while performing sensitive activities, engage in conducts that do not comply with the Model's prescriptions, cause damages or create situations of potential hazard for the Foundation. That behaviour dramatically undermines the Foundation's trust in those workers, with a severe damage for the company.

It is understood that all the provisions and guarantees provided for by the law and by the employment contracts regarding disciplinary measures are to be complied with, specifically:

- before any disciplinary measure is imposed, the employee must be notified of the charge and his defence must be heard;
- except for verbal reprimands, the charge must be in writing and the measure must not be issued until the specific days specified in the employment contracts for each sanction have elapsed, starting from the moment when the charge was notified.

As far as the investigation of the violations, the disciplinary measures and the sanctions imposed are concerned, the powers already conferred upon the Foundation's management remain valid, within the limits of their delegations and powers.

The type and extent of each of the penalties set shall be applied also considering:

- the intentionality of the behaviour or the degree of negligence, recklessness or unskilfulness, with regard to the predictability of the event;
- the overall conduct of that particular worker, with regard to the existence of disciplinary precedents of his/hers, within the limits permitted by the law;
- the worker's tasks;
- the functional position and level of responsibility and autonomy of those involved in the facts constituting the breach;
- other special circumstances surrounding the disciplinary offence.

³ For example, failure to comply with the corporate procedures, failure to provide the Surveillance Body with the prescribed information, failure to perform controls, etc.

It is also envisaged that any retaliatory or discriminatory measure adopted against the reporting party will be proportionally sanctioned. Sanctions are also applied in the event of violations of the measures to protect the privacy of the reporting party.

The person responsible for actually applying the disciplinary measures described above is the head of the relevant organisational unit who, if he/she believes that there is enough evidence for the employee's liability, orders that the disciplinary measures be applied without delay, on his/her own initiative or at the SB's request, and imposes any sanctions recommended by the Surveillance Body, after hearing the perpetrator's direct superior.

Nonetheless, the task of checking and assessing the suitability of the disciplinary system pursuant to the Decree is assigned to the Surveillance Body, in collaboration with the head of the relevant organisational unit.

Measures against executives

If executives violate the prescriptions and behavioural rules contained in the Model, the Foundation shall impose the most suitable disciplinary sanctions on the perpetrators, in compliance with the National Collective Employment Contract for executives of insurance companies.

If the executive violates the Model and/or the internal regulations described therein so seriously as to nullify the relationship of trust with the Foundation, he/she may also be punished with his/her dismissal for just cause.

As envisaged, any retaliatory or discriminatory measure against the whistle-blower shall also be proportionally punished. The penalties also apply to any violations of the measures protecting the privacy of the latter.

Measures against Directors

Upon learning of any violations of the provisions and rules of conduct of the Model by members of the Board of Directors, the Surveillance Body shall promptly inform the whole Board of Directors and the Board of Auditors.

As set forth in the Statute, the recipients of the Surveillance Body's report may take steps to adopt the most suitable measures provided by law and/or revoke any delegations and/or the offices or positions held by those directors.

Measures against members of the Board of Auditors

Upon learning of any violations of the provisions and rules of conduct of the Model by one or more members of the Board of Auditors, the Surveillance Body shall promptly inform all members of the Board of Auditors and the Board of Directors.

As set forth in the Statute, the recipients of the Surveillance Body's report may take the appropriate steps to adopt the most suitable measures provided by law and/or revoke the offices or positions held by those members.

Measures against other Addressees

Every violation of the provisions and rules of behaviour contained in the Model, or the possible perpetration of the crimes covered by the Decree by the third parties with whom the Foundation has contract relationships (such as suppliers, consultants / contractors, trade partners, etc.) is punished according to relevant contract clauses. Those clauses may include, for example, the right to terminate the contract and/or impose the payment of penalties. The levy of sanctions may also imply a prohibition of new contract relationships with those concerned.

In addition, with specific reference to Agents, any violations of the instructions provided in the Circulars to Networks will be punished with specific sanctions. In particular, reference is made to the relevant provisions of Articles 12, paragraph 1 e) and 18 of the ANA (National Agents Agreement) which, among the causes for termination of agency relationships, include the principal's withdrawal for just cause.

5 Update and Adaptation of the Model

It is the responsibility of the Board of Directors to oversee the update and adaptation of the Model, if the circumstances so require and, in any case, whenever the SB urges the Board to do so.

The same Board assigns to the Group's "Legislative Decree 231/01" unit the responsibility to oversee the update of the Model, in collaboration with the other competent structures, and to prepare and update the relevant protocols.

In order to keep the Model effective and efficient over time, it needs to be updated and revised "substantially", should one or more of the following events occur, for instance:

- legislative innovations with reference to the laws on the liability of entities for administrative torts connected with crimes;
- any interpretation of case law and of the relevant prevailing legal theory;
- confirmed shortcomings and/or gaps and/or significant violations of the Model emerging from any assessments of its effectiveness;
- significant changes in the organisational structure or in the lines of activity of the Foundation;
- considerations resulting from the application of the Model, including experiences gained in the criminal litigations in which the Foundation was involved.

Substantial amendments or additions to this Model shall be the responsibility of the Board of Directors of the Foundation, including on the Surveillance Body's recommendation, which, therefore, retains the duties and powers detailed in Chapter 3, paragraph 2 about promoting and monitoring constant updating of the Model.

On the other hand, as regards non-substantial amendments or additions to the Model (e.g. amendments to the existing internal rules, formal changes of the organisational/functional structure), they are the responsibility of the Group's "Legislative Decree 231/01" unit, which is required to inform the Board of Directors.

SPECIAL PART

Foreword

The Special Part is an integral part of the Model that the Foundation has adopted to meet the prevention requirements imposed by Legislative Decree 231/01 (hereinafter also referred to, in short, as “Decree”).

According to article 6, paragraph 1, letter a) of the Decree, the Foundation, by mapping risks and by assessing the activities, the checks in place and the corporate context in which it operates (through the so-called Risk Self-Assessment), has identified the sensitive activities within which the offences described in the Decree may be committed.

In order to prevent or mitigate the risk of those offences being committed, the Foundation, as a result, set out general principles of conduct and general safeguards, which can be applied to all “sensitive” activities, as well as specific safeguards for each of the identified activities at risk.

This Special Part is meant to regulate the conduct of the Addressees of this Model, as indicated in the General Part, more specifically to:

- **highlight** the essential control measures for preventing or mitigating unlawful acts, as transposed in operating procedures and corporate practices, so as to make them fit for preventing the offences stated in the Decree from being committed;
- **provide** the SB and the heads of the other corporate functions who co-operate with it with the operating tools needed to perform their checking, monitoring and verification activities.

How to read the Special Part

Instructions for consulting the document in a swift and effective manner and for ensuring prompt identification of the relevant sensitive activities for each Addressee and of the appropriate management and control tools to be adopted are provided below.

The structure of the Special Part consists of **11** sections:

- Section **A**, regarding offences against the Public Administration (articles 24 and 25 of the Decree) and private-to-private corruption (article 25-ter of the Decree);
- Section **B**, regarding computer crimes (article 24-bis of the Decree);
- Section **C**, regarding organised crime (art. 24-ter of the Decree) and transnational crimes (article 10 of Law no. 146 of 16 March 2006);
- Section **D**, regarding crimes of counterfeiting in currency, legal tender, revenue stamps, and distinctive signs (article 25-bis of the Decree);
- Section **E**, regarding corporate offences (article 25-ter of the Decree);
- Section **F**, regarding crimes of manslaughter and serious or very serious injuries committed in violation of the laws on the protection of health and safety in the workplace (article 25-septies of the Decree);
- Section **G**, regarding crimes such as: handling stolen goods, money-laundering and use of money, goods or assets of unlawful origin, as well as self-laundering (article 25-octies of the Decree) and crimes of terrorism or subversion of the democratic order (article 25-quater of the Decree);
- Section **H**, regarding offences related to copyright violations (article 25-novies of the Decree);
- Section **I**, regarding crimes of instigation not to testify or to give false testimony before court authorities (article 25-decies of the Decree);
- Section **J**, regarding environmental crimes (article 25-undecies of the Decree);
- Section **K**, regarding crimes of employing third-country citizens with irregular work permits (art. 25-duodecies of the Decree), as well as crimes against individuals, included the crimes described in article 603-bis p. c.: “Illicit brokering and labour exploitation” (art. 25-quinquies of the Decree).

The sections are uniformly structured into 5 paragraphs with alternating descriptive parts and summary tables:

- I. Relevant offences for the Foundation;
- II. Identification of sensitive activities;
- III. General principles of conduct;
- IV. Specific control principles for sensitive activities;
- V. Further Control Safeguards;

Paragraph I **Relevant offences for the Foundation** describes the offences that are supposed to apply to the Foundation, based on the outcomes of the Risk Self-Assessment activity, taking as a reference the various categories of predicate offences specified in the Decree.

ID	Descrizione attività sensibile	Funzioni aziendali coinvolte	Reati rilevanti	Esempi di potenziali comportamenti illeciti per reati di RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, AUTORICICLAGGIO
201	Gestione dei pagamenti e delle erogazioni (e.g. inserimento fatture, creazione di ordini di pagamento)	Segreteria Generale	1) Art. 648-bis c.p. Riciclaggio 2) Art. 648-ter c.p. Impiego di denaro, beni o utilità di provenienza illecita 3) Art. 648 c.p. Ricettazione 4) Art. 648-ter 1 c.p. Autoriciclaggio	1) Sostituzione o trasferimento di denaro o altre utilità derivanti da un delitto non colposo, mediante l'incasso ed il successivo reimpiego di denaro/utilità con modalità concretamente idonee ad ostacolare l'identificazione della provenienza illecita 2) Utilizzo di denaro di provenienza illecita per l'erogazione dei finanziamenti per i progetti 3) Utilizzo di denaro per l'acquisto di beni provenienti da delitto 4) L'effettuazione di pagamenti attraverso l'impiego di denaro proveniente da un delitto non colposo che un soggetto apicale o subordinato appartenente alla Fondazione stessa ha commesso o concorso a commettere, in modo da ostacolare concretamente l'identificazione della sua provenienza delittuosa

ESEMPIO

Descrizione dell'attività sensibile a rischio

Funzioni aziendali coinvolte nello svolgimento dell'attività sensibile in oggetto. Il lettore può servirsene per individuare le attività della sua funzione presenti nella sezione che sta consultando

Numero che identifica univocamente l'attività sensibile in tutte le sezioni della Parte Speciale

Questa colonna riporta i reati la cui commissione è stata valutata ipoteticamente possibile nello svolgimento delle attività sensibili in oggetto

In questa colonna il lettore può consultare alcuni esempi di commissione dei reati, ipotizzati al fine di rappresentare alcune possibili condotte illecite che il destinatario deve astenersi dal porre in essere

Paragraph II **Identification of sensitive activities** analyses the sensitive activities which, following the Risk Self-Assessment activity, have been considered potentially at risk for the perpetration of the offences included in I. In particular, the areas, corporate processes and company structures considered “at risk” for the offences in question are specified. The reader may then consult a table containing some basic information about the above activities. A few indications on how to read and best interpret the table are given below:

Paragraph III **General principles of conduct** illustrates the obligations and prohibitions which, in general and as specified in the Group Code of Conduct and in the operating procedures, the Model's Addressees are required to comply with while undertaking the sensitive activities described in the relevant section of the Special Part.

Paragraph IV **Specific control principles for sensitive activities** contains a further table for the Addressees containing specific control safeguards (e.g. GIRS internal regulations, other internal procedures) for each of the above-mentioned activities. Fully outsourced sensitive activities are not included in this table, as each outsourcer has defined its own relevant internal regulations and the other procedures.

ID	Descrizione attività sensibile	Funzioni aziendali coinvolte	Presidi specifici di controllo	
			Normativa interna rilevante	Altre procedure interne
201	Gestione dei pagamenti e delle erogazioni (e.g. inserimento fatture, creazione di ordini di pagamento)	Group Chief Financial Officer / Group Corporate Finance / Group treasury	- Group Anti-Money Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	

ESEMPIO

Numero che identifica univocamente l'attività sensibile in tutte le sezioni della Parte Speciale.

Descrizione dell'attività sensibile a rischio

Funzioni aziendali coinvolte nello svolgimento dell'attività sensibile in oggetto. Il lettore può servirsene per individuare le attività della sua funzione presenti nella sezione che sta consultando

Descrizione dei presidi specifici di controllo: il lettore può servirsi di queste colonne per individuare la normativa interna (e.g. normativa GIRS, Protocolli) e le altre procedure interne (e.g. istruzioni operative, manuali interni) a cui si deve attenere nello svolgimento delle attività sensibili

Paragraph **V Further Control Safeguards** illustrates further control safeguards with which Model's addressees must comply while performing their sensitive activities (e.g. operating practices that have not been formalised into documents, system blocks, reports of the Internal Audit function).

Finally, it should be remarked that in some sections the Addressees may find further paragraphs than those listed above, which are related to the specific characteristics of the individual types of crimes. As an example, section A (offences against Public Administration and private-to-private corruption) is introduced by a short illustration of a few key notions connected with Public Administration (definition of public service, public official, etc.).

Section **F** (crimes of manslaughter and serious or very serious injuries committed in violation of the laws on the protection of health and safety in the workplace) takes a partially different approach than that used to regulate other forms of offence: that difference lies in the fact that that sector in question is characterised by the existence of a large number of provisions covering both the mechanisms for identifying duties of care, and the type and contents of precautionary safeguards. The peculiarity of the regulatory environment, as a result, has made it necessary to construct a specific structure that is not described in this guide.

SECTION A – OFFENCES AGAINST THE PUBLIC ADMINISTRATION AND PRIVATE-TO-PRIVATE CORRUPTION

A 1. INTRODUCTION

The notion of Public Administration in criminal law is interpreted in a broad sense, embracing the entire activity of the State and of the other public authorities; as a result, crimes against the Public Administration include deeds that obstruct or perturb the smooth running, not only of the administrative activity – technically speaking, but also of the legislative and judicial activity. Therefore, Public Administration, meant as the totality of the public functions of the State or of other public authorities, is safeguarded.

In order to apply this Model, the notion of Public Administration needs to include:

- the State and all its ramifications, local public authorities and other non-economic public authorities⁴;
- the subjects falling under the definition of “public official” or of “official in charge of a public service” according, respectively, to articles 357 and 358 p. c.⁵, i.e. those who - whether employees of either public or private entities - perform “a public legislative or judicial function” or even “an administrative function” as regulated by public law or by acts exercising of public authority and characterised by the shaping and expression of the Public Administration’s will, possibly through authority and certification powers.

The following non-exhaustive examples fall within the notion of Public Administration:

- State administrations, Ministries, State companies and administrations with autonomous status, regions, provinces, municipalities and the consortia and associations, universities, chambers of commerce, industry, handicraft and agriculture, national, regional and local non-economic public authorities, national healthcare service centres and agencies, INPS (national institute of social insurance), INAIL (national institute for insurance against industrial accidents), labour inspectorate, ASL (local health authorities), Revenue Office, Armed and Police Forces (Carabinieri, Guardia di Finanza (finance police), NAS (food law enforcement), Police, Judicial Police, Capitaneria di Porto (harbour master’s offices), customs authorities, etc.), courts, Civil Registrar’s Offices, Registers of Companies, etc.;
- Subjects who fulfil a public legislative function, such as:
 - Members of Parliament and government officials;
 - regional and provincial councillors;
 - MEPs and members of the Council of Europe;
 - individuals who perform ancillary functions (who are responsible for keeping parliamentary documents and records, as well as preparing stenographic, bursar’s, technical reports, etc.);
- Subjects who occupy a public judicial post, such as:
 - magistrates (ordinary magistrates in Courts, Courts of Appeal, Court of Cassation, High Court of Public Waters, Regional Administrative Courts (TARs), Council of State, Constitutional Court, Military Courts, wing members of courts of assizes, justices of the peace, members of formal arbitration panels and of parliamentary enquiry committees, magistrates of the Court of Justice of the European Union, as well as of a number of international courts, etc.);
 - subjects who perform related functions (judicial police officers and agents, Guardia di Finanza (finance

⁴ Symptomatic indices for identifying “bodies governed by public law” according to the interpretation of EU law are:

- a legal person, also organised as a corporation;
- being subject to the State’s surveillance and control or having more than half of the members of the administrative and supervisory bodies who are designated by the State or local authorities, or being mainly funded by the State or public authorities;
- carrying out activities without any cost-effectiveness criteria (economic risk borne by the State), pursuing neither industrial nor commercial goals, but in the public interest.

⁵ According to article 357 p. c. a public official is “anyone who fulfils a public legislative, judicial or administrative function”, specifying that “the administrative function is public when it is governed by public law and by acts constituting the exercise of public authority and is characterized by the shaping and expression of the will of the Public Administration and by its unfolding by way of public authority and certifying powers”. Therefore, public officials are identified as those who, in their capacity as public or private sector employees, can or must shape and express the will of the Public Administration, or exercise public authority or certifying powers under public law.

According to article 358 p. c., officers in charge of a public service are “those individuals who, in any capacity, render a public service”, the latter being understood as “an activity governed in the same ways as a public function, but characterized by the lack of the typical powers of the latter, except for simple duties and works of a merely material nature”. Therefore, those officers provide a public service but are not endowed with the same powers of public officials, i.e., although acting within an activity regulated as a public function, do not exercise the typical powers of the latter and perform neither simple duties, nor works of a merely material nature.

police) and Carabinieri, court clerks, secretaries, bailees, bailiffs, witnesses, conciliation messengers, authorised liquidators, clerks issuing certificates at court clerks' offices, experts and consultants for Public Prosecutors, liquidators in arrangements with creditors, liquidators of compositions with creditors, liquidators of large companies in crisis under special administration, etc.);

- Subjects who occupy a public administrative post, such as:
 - employees of the State, of international and foreign bodies, of local bodies (e.g. officials and employees of the State, of the European Union, of supranational bodies, of foreign States and of local authorities, including regions, provinces, municipalities, and mountain communities; subjects performing ancillary functions, as opposed to the State's institutional purposes, such as members of municipal technical offices, members of territory adjustment councils, administrative heads of tax amnesty offices, municipal ushers, clerks dealing with files related to occupying public places or land, municipal employees working at employment services offices, employees of State-owned companies and municipal utilities; subjects responsible for collecting taxes, healthcare personnel in public structures, staff of Ministries, *Soprintendenze* (i.e. Boards for Cultural Heritage and Preservation), etc.
 - employees of other public bodies, either national or international (e.g. officials and employees of Chambers of Commerce, of the Bank of Italy, of Supervisory Authorities, of social security agencies, ISTAT (the Italian national statistics institute), of the UN, FAO, etc.);
- private individuals who exercise public functions or provide public services (e.g. employees of private entities operating as concession holders or whose activities are however governed by public law, or carrying out activities of public interest, or being controlled in whole or in part by the State, etc.).

Furthermore, for the purposes of applying this Model to Supervisory Authorities, reference should be made to all entities endowed with a particular autonomy and impartiality whose goal is to protect some constitutionally significant interests, such as the proper functioning of Public Administration, free competition, the protection of professional confidentiality, etc., including but not limited to: Bank of Italy, Consob, UIF, AGCM, Italian Data Protection Authority, AGCOM, etc.

Finally, it should be noted that the Risk Self-Assessment activity has detected a high level of homogeneity between the sensitive activities considered potentially at risk of private-to-private corruption and of instigating that kind of corruption, as compared to those identified as potentially relevant for committing corruption offences, in a broad and general sense, affecting the Public Administration. Against this background, in order to draw up an Organisation Model that is as clear, effective and usable as possible for the Addressees of this Model in the mapping out of risks of committing the offences indicated by the Decree, the Foundation has deemed it appropriate to represent the sensitive activities considered to be at risk of corruption offences both against the Public Administration and between private parties in a unified way within this Section A.

A 2. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the Foundation's activities proved exposed to the risk of commission of relevant offences in its relationships with the Public Administration, which are briefly described below, as they are referred to in Articles 24 and 25 of the Decree, as well as offences of private-to-private corruption and instigation thereto, as specified in article 25-ter of the Decree, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Offences against the Public Administration

Embezzlement against the State, as provided for in article 316-bis p. c., consisting in the conduct of any one who – while not being part of the Public Administration, after receiving contributions, subsidies or funds for initiatives aimed at implementing public works projects or activities of public interest from the State, from any other public body, or from the EU, fails to allocate them for the above purposes.

Misappropriation to the detriment of the State, as provided for in article 316-ter p. c., consisting in the conduct of individuals who – except when the offence falls within article 640-bis p. c. – by using or submitting statements or documents that are either false or vouch for things that are false, or by failing to provide required information, obtain – for themselves or for others – undue contributions, financing, subsidised loans, or other similar funds, whatever their name, from the State, from other public bodies or from the EU.

Fraud against the State or another public body, provided for in article 640, paragraph 2, no. 1 p. c., consisting in the conduct of anyone who, with artifices or deception, by misleading somebody, reaps an unfair advantage for themselves or others, while causing damage to third parties, if the offence is committed to the detriment of the State or of any other public body, or under the pretext of exempting someone from military service.

Aggravated fraud for the appropriation of public funds, as provided for in article 640-bis p. c., consisting in the same conduct as described in the previous item, if entertained in to obtain contributions, funds, subsidised loans or other

disbursements of the same kind, whatever their names, which are granted by the State, other public bodies or by the EU.

Computer fraud, as provided for in article 640-ter p. c., consisting in the conduct of anyone who, by tampering in any way with the operation of a computer or Internet-based system or by unduly affecting in any way data, information or programs contained in a computer or Internet-based system, makes unfair gains for themselves or others, while causing damage to others.

Extortion, as provided for in article 317 p. c., consisting in the conduct of public officials or of officials exercising a public service who, by abusing their capacities or powers, force someone to unduly give or promise, to them or third parties, money or other benefits.

Corruption in the exercise of one's function, as provided for in article 318 p. c., consisting in the conduct of public officials who, while performing actions lying within their functions, receive, for themselves or for third parties, an undue remuneration in cash or as other benefits, or accept a promise of such advantages.

Corruption for acts in breach of official duties, as provided for in article 319 p. c., consisting in the conduct of public officials who, for omitting or delaying or for having omitted or delayed deeds of their offices, or for performing or having performed acts in breach of their official duties receive, for themselves or for third parties, cash or other benefits, or accept a promise thereof.

Aggravating circumstances, as provided for in article 319-bis and relating to the offence of corruption for acts in breach of official duties concerning the awarding of public-sector employment, salaries or pensions or the conclusion of contracts involving the administration to which the public official belongs, as well as the payment or refund of taxes.

Judicial corruption, as provided for in article 319-ter, paragraph 2 p. c., consisting in cases of corruption while exercising official functions or for acts in breach of official duties, if committed to favour or damage one party in a civil, criminal or administrative proceeding.

Unlawful inducement to give or promise any benefits, as provided for in article 319-quater p. c., consisting in the conduct of public officials who, by abusing their capacities or their powers, induce someone to unlawfully give or promise to them or third parties, cash or other benefits.

Bribery of an official in charge of a public service, as provided for in article 320 p. c., consisting in the conduct referred to in article 319 p. c., if committed by the person in charge of a public service, as well as by the conduct referred to in article 318 p. c., if the offender is a person in charge of a public service and a civil servant.

Penalties for bribers, as provided for in article 321 p. c., which states that the penalties envisaged by articles 318, (paragraph 1), 319, 319-bis, 319-ter and 320 also apply to those who give or promise money or other benefits to public officials or officials in charge of public services.

Instigation to corruption, as provided for in article 322 p. c., consists in the conduct of anyone who offers or promises undue money or other benefits to public officials or to officials in charge of public services in their capacities as civil servants, to induce them to perform official acts, if the offer or promise is not accepted.

Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States are envisaged in article 322-bis p. c., according to which articles 314, 316 to 320 and 322, paragraphs 3 and 4, p. c. also apply:

- 1) to members of the EU Commission, of the European Parliament, of the Court of Justice and of the Court of Auditors of the European Union;
- 2) to officials and servants hired by contract under the Staff Regulations of Officials of the European Union or under conditions of employment of other servants of the European Union;
- 3) to people seconded by the Member States or by any other public or private body of the European Union who fulfil functions corresponding to those of EU officials or servants;
- 4) to members and personnel of bodies set up according to the Treaties establishing the European Communities;
- 5) to those individuals who, within other Member States of the European Union, perform functions or activities corresponding to those of public officials and of officials in charge of public services.

The above people are treated as public officials, if they exercise corresponding functions, and as officials in charge of public services in the remaining cases.

The provisions of article 322, paragraphs 1 and 2, p. c. also apply if the cash or other benefits are given, offered or promised:

- 1) to the subjects listed below:
 - o members of the EU Commission, of the European Parliament, of the Court of Justice and Court of Auditors

- of the European Union;
 - officials and servants hired by contract under the Staff Regulations of Officials of the European Union or under conditions of employment of other servants of the European Union;
 - people seconded by the Member States or by any other public or private body of the European Union who fulfil functions corresponding to those of EU officials or servants;
 - members and personnel of bodies set up according to the Treaties establishing the European Communities;
 - those individuals who, within other Member States of the European Union, perform functions or activities corresponding to those of public officials and of those in charge of public services;
- 2) individuals who fulfil functions or perform activities corresponding to those of public officials or of people in charge of public services in foreign States or international organisations, if the offence is committed in order to grant themselves or others unlawful advantages in international economic operations or to obtain or maintain an economic or financial activity.

Offences of private-to-private corruption and of instigation to private-to-private corruption

Private-to-private corruption, limited to the offence provided for in article 2635, paragraph 3 c. c. (so-called active bribery), consists in the conduct of those who, even through third parties, offer, promise or give undue cash or other benefits to directors, general managers, executives in charge of preparing corporate accounting records, auditors and liquidators of companies or private entities (who solicit, receive or accept them) to perform or to omit an action in breach of the obligations inherent in their office or of their loyalty obligations.

This offence also applies if committed against those who, within the organisation of the company or private organisation, exercise different managerial functions from those of the subjects indicated above.

Instigation to private-to-private corruption, limited to the circumstances provided for in article 2635-bis p. c. consisting in the conduct of anyone who offers or promises undue cash or other benefits to administrators, general managers, executives in charge of preparing corporate accounting documents, auditors and liquidators of companies or private entities, as well as those who perform managing activities within them, so that they perform or omit an act in breach of the obligations of their office or of their loyalty obligations, whenever the promise or offer is not accepted.

A 3. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk Self-Assessment activity, the Foundation has identified sensitive activities during which some of the offences against the Public Administration envisaged by articles 24 and 25 of the Decree might be committed, in addition to the offences of private-to-private corruption and instigation thereto, as envisaged by article 25-ter of the Decree .

The sensitive activities identified within the Risk Self-Assessment, and shown in a table with a description of each activity, of the corporate functions involved, of the relevant offences against the Public Administration, as well as examples of potential illegal conducts, both with regard to offences against the Public Administration and to offences of private-to-private corruption are listed below. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
1	Preparation and management of the budget for financing plans for the projects supported by the Foundation, as well as approval of extra-budgets	General Secretariat	1) Activity instrumental in committing one of the following offences: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in breach of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of public services • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Preparation and management of the cost budget for funding projects so as to better conceal subsequent abnormalities that might be indicative, for instance, of off-balance-sheet funds set up for bribing members of the Public Administration.	3) Preparing and managing cost budgets for funding projects so as to better conceal subsequent abnormalities that might be indicative, for instance, of off-balance-sheet funds set up for bribing purposes
2	Verification of the assessment process of entities receiving charitable contributions	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Fake checks on the evaluation process of the recipient bodies of charitable contributions aimed at facilitating the choice of a specific partner as a form of benefit for Public officials / officials in charge of Public Services or for individuals close to or appreciated by them.	3) Fake checks on the evaluation process of the recipient bodies of charitable contributions aimed at facilitating the choice of a specific partner as a form of benefit for representatives of private foundations or individuals close to or appreciated by them.

⁶ The examples of unlawful conduct concerning private-to-private corruption shown in the table refer to such crimes as laid down in articles 1) 2635 and 2) 2635-bis c. c. and 3) to all activities that are instrumental in committing those offences.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
3	Approval of charitable contributions	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Approval of charitable contributions for financing projects without the applicable requirements as a form of benefit for Public Officials / Officials in charge of Public Services or for individuals close to or appreciated by them.	3) Approving charitable contributions for financing projects without the applicable requirements as a form of benefit for representatives of private foundations or for individuals close to or appreciated by them.
4	Monitoring projects funded by the Foundation	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Failure to detect anomalies or inadequate management of those identified in the management of projects funded by the Foundation as a form of benefit for Public Officials / Officials in charge of Public Services or for individuals close to or appreciated by them.	3) Failing to detect anomalies or inadequate management of those identified in the management of projects funded by the Foundation as a form of benefit for representatives of private foundations or for individuals close to or appreciated by them.

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
5	Marketing - Management of gifts	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Promising and/or offering goods as gifts or discretionary discounts, of no small value, to Public Officials, Officials in charge of Public Services or any person designated by them, also together with others, in order to obtain undue favourable treatment in any business activity and, more generally, for corruption purposes (e.g. to obtain public funding that would be otherwise inaccessible)	3) Unduly conditioning, with gifts, a representative (or an associated) of a foundation supplying goods or services, in order to obtain favourable measures (e.g. in order to obtain supplies at otherwise uncompetitive prices)
7	Management of public relationships (including with public figures) and communication and marketing activities (advertising, promotional events, media corners, sponsorships, etc.)	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Activity instrumental in committing one of the offences in items 1) to 7)	1/2/3/4/5/6/7/8) Through undue pressure, within the management of relationships with subjects of public relevance (national, regional, municipal) while participating in events and/or sponsorships and/or marketing activities, exercising lobbying for business-related law regulations in order to favour specific interests and obtain advantages for the Foundation	1/2) Offering money to representatives of other insurance companies to convince them to engage in lobbying in order to obtain advantages related to the promotion of business. 3) Exercising advertising activities, including unprofitable ones, in order to obtain particular advantages from the financed organisation.

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
8	Selection of bodies receiving charitable contributions	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Selection of recipient entities as a form of benefit for Public Officials / Officials in charge of Public Services or individuals close to or appreciated by them.	3) Selecting recipient entities as a form of benefit for representatives of a private foundation or individuals close to or appreciated by them.
9	Managing relations with partners identified for the management of the Foundation's projects	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter p. c. Judicial corruption • Art. 319-quater p. c. Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Art. 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Concluding fake agreements in order to create off-balance sheet funds for corruption purposes	3) Concluding fake agreements in order to create off-balance sheet funds for corruption purposes

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
10	Management of reports for expenses, travelling and entertaining expenses	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Providing fake reimbursements of expenses to employees to create financial resources in their names to be used for corruption purposes.	3) Providing fake reimbursements of expenses to employees to create financial funds in their names to be used for corruption purposes. As a non-exhaustive example, the offence in question may be committed if the Head and/or an employee of the Organisational Unit, through fake expense reports, generates concealed cash reserves in order to bribe third representatives or employees of a legal person, so that they perform or omit acts, in violation of their office obligations or loyalty obligations, in order to obtain improper advantages for the Foundation.
16	Relations with representatives of the Public Administration in the context of the management of regulatory and administrative formalities, also through external subjects (e.g. notices to offices of Municipalities and Provinces, to the Revenue Office, to Tax Offices, to INPS, INAIL, filing of powers of attorneys, of balance sheets, and of minutes, etc.)	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Article 640, paragraph 2 p. c. Bribery against the State or another Public Body	1/2/3/4/5/6/7) Giving or promising money or other benefits to public officials to have them ignore delays, omissions or mistakes made in communications, or omit / mitigate any penalties imposed after any checks 8) Producing false documentation for the Financial Administration concerning the Foundation and the required formalities so as to mislead the Public Administration in order to obtain funds In the management of administrative formalities concerning staff, mislead the State or a public authority (e.g. INPS) by submitting false or altered documents, thus reaping unfair gains (e.g. contributory reliefs for mandatory hiring), and damaging the public authority.	

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
17	Relationships with Public Administration representatives within their inspection and control activities, as well as recording and acquisition of their findings (for example: Revenue Office, Guardia di Finanza, INPS, INAIL, labour inspectorate, ISPEL, SPISAL, Provincial Labour Directorate, Data Protection Authority, ISTAT, chambers of commerce, ASL, Fire Brigades, foreign authorities, etc.)	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1/2/3/4/5/6/7) Giving or promising money or other benefits to the Head of the Provincial Fire Brigade so as to speed up the renewal procedure of the fire prevention certificate. During an inspection, giving or promising money or other benefits to a Labour Inspector to convince him/her not to include any irregularities detected in his/her assessment report. Giving or promising money or other benefits to the Head of the Provincial Fire Brigade in order to renew the fire prevention certificate, although the relevant regulatory requirements are not met.	
18	Management of the penalties imposed by the administrative authority (reception and verification of the penalties, allocation of the sums needed to cover any expenses to be incurred for the penalties).	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Article 640, paragraph 2, c. c. Fraud against the State or other Public Authority	1/2/3/4/5/6/7) Giving or promising money or other benefits to a representative of the Public Administration to convince him/her to cancel a penalty so as to grant an undue advantage to the Foundation 8) Fraudulent management of obligations regarding the payment of penalties in order to create an advantage for the Foundation, to the detriment of the Public Administration.	

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
19	Search and selection of suppliers	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Selection of suppliers indicated or appreciated by Public Officials or Officials in charge of a public service as a form of benefit intended to make them perform, in the interest of the Foundation, an act in compliance with or in breach of their official duties (e.g. in order to obtain authorisations / concessions without meeting the requirements) 1) Establishment of contacts with suppliers in order to enter into "fake" contracts, instrumental in creating concealed funds, which are not recorded in general accounting ledgers, to be used for bribing members of the Public Administration.	3) Selecting suppliers indicated or appreciated by a representative of a third-party company in order to influence the performance or omission of acts in the interests or for the benefit of the Foundation (e.g. obtaining goods at prices significantly lower than their market value, etc.) 3) Establishing contacts with suppliers in order to enter into "fake" contracts, instrumental in creating concealed funds, which are not recorded in general accounting ledgers, to be used for bribing private subjects
21	Management of the awarding of supply contracts for goods and/or services (tender / direct negotiation)	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Preparation of particularly favourable contracts with suppliers appreciated by representatives of the Public Administration, as a form of benefit in order to obtain an undue advantage from them (e.g. to be awarded a public tender) Deliberate mismanagement of requests for purchase in order to set create off-balance-sheet funds for corrupting Public Administration for the benefit of the Foundation	1/2) Offering or promising money or other benefits to a representative of a foundation supplying goods or services in order to negotiate a price lower than the market price or more favourable purchase conditions for the Foundation (e.g. payment extensions) 3) Deliberately mismanaging requests for purchase in order to set up off-balance-sheet funds for bribing private subjects for the benefit of the Foundation 1/2) Offering or promising money or other benefits to a representative of a foundation supplying goods or services in order to negotiate a price lower than the market price or more favourable purchase conditions for the Foundation (e.g. payment extensions) 3) Deliberately mismanaging requests for purchase in order to set up off-balance-sheet funds for bribing private subjects for the benefit of the Foundation

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
22	Preparation, conclusion and transmission of a contract/purchase order	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Preparing particularly favourable contracts with suppliers appreciated by representatives of the Public Administration, as a form of benefit to gain an undue advantage from them (e.g. to be awarded a public tender) Deliberate mismanagement of requests for purchase in order to set up off-balance-sheet funds for bribing representatives of Public Administration for the benefit of the Foundation	1/2) Offering or promising money or other benefits to a representative of a foundation supplying goods or services in order to negotiate a price lower than the market price or more favourable purchase conditions for the Foundation (e.g. payment extensions) 3) Deliberately mismanaging requests for purchase in order to create off-balance-sheet funds for bribing private subjects for the benefit of the Foundation 1/2) Offering or promising money or other benefits to a representative of a foundation supplying goods or services in order to negotiate a price lower than the market price or more favourable purchase conditions for the Foundation (e.g. payment extensions) 3) Deliberately mismanaging requests for purchase in order to set up off-balance-sheet funds for bribing private subjects for the benefit of the Foundation
23	Designation and monitoring of suppliers	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Qualification and monitoring of suppliers indicated or appreciated by representatives of the Public Administration as a form of benefit to obtain in exchange an undue advantage for the Foundation Establishment of contacts with suppliers in order to enter into "fake" contracts, instrumental in creating concealed funds, not recorded in general accounting ledgers, to be used for bribing members of the Public Administration. 1) Qualification and monitoring of suppliers indicated or appreciated by representatives of the Public Administration as a form of benefit to obtain in exchange an undue advantage for the Foundation Establishment of contacts with suppliers in order to enter into "fake" contracts, instrumental in creating concealed funds, not recorded in general accounting ledgers, to be used for bribing members of the Public Administration	3) Selecting suppliers linked to a representative of a third-party company in the interest or for the benefit of the Foundation (e.g. obtaining goods at prices significantly lower than their market value, etc.) Establishing contacts with trustees in order to enter into "fake" contracts, instrumental in creating concealed funds, not recorded in general accounting ledgers, for bribing private subjects

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
24	Receiving goods and services and authorising payments	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Approval of the payment of invoices to suppliers who are appreciated or indicated by Public Administration representatives for non-existent or lower value services, as a form of benefit to obtain undue advantages for the Foundation Approval of the payment of invoices for non-existent (in whole or in part) services, in order to create unaccounted funds to be used for bribing Public Administration representatives	1/2) Approving the payment of invoices to suppliers who are appreciated or indicated by representatives of private organisations for non-existent or lower value services, as a form of benefit to obtain undue advantages for the Foundation 3) Approving the payment of invoices for non-existent (in whole or in part) services in order to create unaccounted funds for bribing private subjects
25	Management of suppliers' master data	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Alteration of master data of both actual and fake suppliers in order to create off-balance sheet funds for corruption purposes and/or to grant benefits to Public Administration representatives	3) Altering master data of both actual and fake suppliers in order to establish off-balance sheet funds to devote to corruption and/or to grant benefits to private subjects

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
26	Designation and monitoring of IT outsourcers	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Qualification and monitoring of outsourcers indicated or appreciated by representatives of the Public Administration as a form of benefit to obtain an undue advantage for the Foundation Establishment of contacts with outsourcers in order to enter into "fake" contracts, which are instrumental in creating concealed funds, not recorded in general accounting ledgers, to be used for bribing members of the Public Administration.	1/2) Selecting suppliers linked to a representative of a third-party company in the interests or for the benefit of the Foundation (e.g. obtaining goods at prices significantly lower than their market value, to the company's detriment, etc.) 3) Establishing contacts with trustees in order to enter into "fake" contracts, instrumental in creating concealed funds, not recorded in general accounting ledgers, to be used for bribing private subjects
27	Designation and monitoring of administrative outsourcers	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Qualification and monitoring of trustees indicated or appreciated by representatives of the Public Administration as a form of benefit to obtain an undue advantage for the Foundation in exchange Establishment of contacts with trustees in order to enter into "fake" contracts, instrumental in creating concealed funds, not recorded in general accounting ledgers, to be used for bribing members of the Public Administration.	1/2) Offering or promising money or other benefits to a representative of a Foundation supplying goods or services in order to negotiate a price lower than the market price or more favourable purchase conditions for the Foundation (e.g. payment extensions) 3) Deliberately mismanaging requests for purchase in order to set up off-balance-sheet funds for bribing private subjects for the benefit of the Foundation

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
28	Preparation and transmission of purchase requests	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Preparation of particularly favourable contracts with suppliers appreciated by representatives of the Public Administration, as a form of benefit to obtain an undue advantage from them (e.g. to be awarded a public tender) Deliberate mismanagement of requests for purchase in order to create off-balance-sheet funds for bribing representatives of the Public Administration for the benefit of the Foundation	1/2) Offering or promising money or other benefits to a representative of a Foundation supplying goods or services in order to negotiate a price lower than the market price or more favourable purchase conditions for the Foundation (e.g. payment extensions), thereby causing damage to the supplying foundation itself 3) Deliberately mismanaging requests for purchase in order to create off-balance-sheet funds for corruption purposes for the benefit of the Foundation
29	Conclusion of passive lease contracts	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Conclusion of contracts at unfavourable conditions for the Foundation as a form of benefit to Public Administration representatives in order to obtain other undue advantages for the Foundation Conclusion of contracts in order to create concealed funds, not duly entered in general ledgers, to be used for bribing public subjects	3) Concluding contracts at unfavourable conditions for the Foundation as a form of benefit to representatives of private organisations in order to obtain other undue advantages for the Foundation Concluding contracts in order to create concealed funds, not duly entered in general ledgers, to be used for bribing private subjects

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
30	Conclusion of active rental / lease contracts	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Conclusion of contracts at unfavourable conditions for the Company as a form of benefit to Public Administration representatives in order to obtain undue advantages Conclusion of contracts with third parties in order to create concealed funds, not duly entered in general ledgers, to be used for corruption of the Public Administration	3) Concluding contracts at unfavourable conditions for the Foundation as a form of benefit to private organisations representatives in order to obtain other undue advantages for the Foundation Concluding contracts in order to create concealed funds, not duly entered in general ledgers, to be used for bribing private subjects
31	Management of scheduled and unscheduled, ordinary and extraordinary maintenance operations	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Mismanagement of maintenance operations as a form of benefit to Public Administration representatives (e.g. selection of maintenance technicians appreciated by the above subjects) Fraudulent management of maintenance operations to set up concealed funds, not entered in general ledgers, to be used for corruption purposes (e.g. by overestimating the costs of the maintenance operation)	3) Mismanaging maintenance operations as a form of benefit to third parties (e.g. selection of maintenance technicians appreciated by third parties) Fraudulently managing maintenance operations to set up concealed funds, not appearing in general ledgers, to be used for corruption purposes

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
32	Management of compliance and upgrading activities of real estate properties	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Activity instrumental in committing one of the offences described in items 1) to 7)	1/2/3/4/5/6/7) Offering money, goods or other benefits to a public official / official in charge of a public service in order to obtain favourable deeds / certifications / measures to make a property compliant with current laws, including in absence of legal requirements 8) Mismanagement of maintenance operations as a form of benefit to Public Administration representatives (e.g. selection of maintenance technicians appreciated by the above individuals) Fraudulent management of maintenance operations to set up concealed funds, not appearing in general ledgers, to be used for corruption purposes	3) Mismanaging maintenance operations as a form of benefit to Public Administration representatives (e.g. selection of maintenance technicians appreciated by the above subjects) Fraudulently managing compliance requirements to set up concealed funds, not appearing in general ledgers, to be used for corruption purposes
33	Administrative management of rental/lease contracts (e.g. renewal, amendment, termination etc.)	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Conclusion of fake contracts with third parties in order to set up concealed funds, not duly entered in general ledgers, to be used for corruption purposes Conclusion of a lease contract for an asset with Public Administration representatives at a price lower than the market price in order to receive preferential treatment.	3) Concluding fake contracts with third parties in order to set up concealed funds, not duly entered in general ledgers, to be used for bribing the Public Administration Concluding a lease contract for an asset to third parties at a price lower than the market price in order to receive preferential treatment.

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
37	Selection and assignment of files to external lawyers	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Assigning files to external lawyers who are appreciated by Public Administration representatives as a form of benefit	3) Assigning files to external lawyers who are appreciated by representatives of third-party companies for corruption purposes, in order to gain an advantage / benefit later on
38	Definition of settlement agreements	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Accepting settlements, although unfavourable to the Foundation, as a form of benefit to Public Administration representatives	3) Accepting settlements, although unfavourable to the Foundation, as a form of benefit to representatives of third-party companies

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
39	Management of in and out-of-court litigations (civil, criminal, administrative, labour law cases)	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Activity instrumental in committing one of the offences described in items 1) to 7)	1/2/3/4/5/6/7) Offering money to a judge (or expert, or arbitrator, or court clerk, or witness) to favourably steer the outcome of a trial 8) Accepting an out-of-court resolution of a dispute, albeit unfavourable to the Foundation, as a form of benefit to Public Administration representatives	1/2) Offering money to a representative of a third-party company to convince him/her to accept the out-of-court settlement of a dispute, albeit unfavourable to the third-party company itself 3) Accepting an out-of-court resolution of a dispute, albeit unfavourable to the Foundation, as a form of benefit to private parties
40	Management of current accounts (opening, closing, changing specimens of signature, etc.)	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Activity instrumental in committing one of the offences described in items 1) to 7)	1/2/3/4/5/6/7/8) Instrumental assignment of the powers to manage current accounts in order to use the funds available for corruption purposes for the Foundation's benefit, including through a third party	Instrumentally assigning the powers to manage current accounts in order to use the available funds for corruption purposes for the Foundation's benefit

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
41	Management of payments and disbursements (e.g. entering invoices, creating claims for payment)	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Activity instrumental in committing one of the offences described in items 1) to 7)	1/2/3/4/5/6/7) Preparation of undue claims for payment to a Public Administration representative, or to a subject appreciated by the latter, for corruption purposes 8) Purposefully incorrect management of collections in order to set up off-balance-sheet funds for corruption purposes for the Foundation's benefit	1/2) Preparing claims for payment to a representative of a third-party company for corruption purposes 3) Purposefully incorrectly managing collections in order to set up off-balance-sheet funds for corruption purposes for the Foundation
42	Management of petty cash	General Secretariat	1) Article 318 p. c. Bribery with the intent to influence an official act 2) Article 319 p. c. Bribery for an act in violation of official duties 3) Article 319-ter p. c. Judicial corruption 4) Article 319-quater p. c. Unlawful inducement to give or promise any benefits 5) Article 320 p. c. Bribery of an official in charge of a public service 6) Article 322 p. c. Instigation to bribery 7) Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 8) Activity instrumental in committing one of the offences described in items 1) to 7)	1/2/3/4/5/6/7) Preparation of undue claims for payment to a Public Administration representative, or to a subject appreciated by the latter, for corruption purposes 8) Purposefully incorrect management of collections in order to set up off-balance-sheet funds for corruption purposes for the Foundation's benefit	1/2) Preparing claims for payment to a representative of a third-party company for corruption purposes 3) Purposefully incorrectly managing collections in order to set up off-balance-sheet funds for corruption purposes for the Foundation's benefit

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
43	Preparation of reports and statements	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Management control analyses aimed at facilitating covering unusual situations that may be indicative, for instance, of off-balance-sheet funds created for corruption purposes	3) Fraudulently producing reports and records to allow setting up, for example, off-balance sheet funds to be used for corruption purposes
44	Administrative management of staff (e. g. processing of payroll slips, calculation of taxes and contributions, etc.)	General Secretariat	1) Activity instrumental in committing one of the offences of: <ul style="list-style-type: none"> • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States 	1) Alteration of data regarding presence/absence/holidays/sick leaves/accidents, of both actual and fake employees, in order to set up off-balance sheet funds for corruption purposes and/or to grant benefits to Public Administration representatives Granting increased salaries than due in order to set up off-balance sheet funds to devote to corruption and/or to grant benefits to Public Administration representatives	3) Altering the data on presence/absence/holidays/sick leaves/accidents, of both actual and fake employees, in order to set up off-balance sheet funds for corruption purposes and/or to grant benefits to a representative of a private foundation or to a subject close to or appreciated by him/her. Granting increased salaries than due in order to set up off-balance sheet funds to devote to corruption and/or to grant benefits to representatives of a private foundation or to a subject close to or appreciated by them

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
45	Processing of contributory, social security and nursing statements	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Alteration of the statements for social security and nursing contributions of both actual and fake employees, in order to set up off-balance sheet funds to devote to corruption purposes and/or to grant benefits to Public Administration representatives	3) Alteration of the statements regarding social security and nursing contributions of both actual and fake employees, in order to set up off-balance sheet funds for corruption purposes and/or to grant benefits to private subjects
48	Accounting and reporting of the Foundation's activities in accounts, evaluations and budget estimates	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Management control analyses aimed at facilitating the concealment of anomalous situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes	3) Fraudulent accounting and reporting of the Company's activities in order to facilitate the concealment of anomalous situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
49	Approval of the financial statements	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Approving the financial statements despite abnormal situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes	3) Approving the financial statements despite abnormal situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes
50	Management of activities connected with drawing up individual financial statements (information sheets, financial statement, and annexes).	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Management control analyses aimed at facilitating the concealment of abnormal situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes	3) Management control analyses aimed at facilitating the concealment of abnormal situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences against the PUBLIC ADMINISTRATION	Examples of potential unlawful conduct for offences of PRIVATE-TO-PRIVATE CORRUPTION ⁶
51	Preparation of the financial statements	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Drawing up the financial statements so as to facilitate the concealment of unusual situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes	3) Drawing up the financial statements so as to facilitate the concealment of unusual situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes
52	Keeping the compulsory registers and books and the financial report	General Secretariat	1) Activity instrumental in committing one of the offences of: • Article 318 p. c. Bribery with the intent to influence an official act • Article 319 p. c. Bribery for an act in violation of official duties • Art. 319-ter Judicial corruption • Art. 319-quater Unlawful inducement to give or promise any benefits • Article 320 p. c. Bribery of an official in charge of a public service • Article 322 p. c. Instigation to bribery • Article 322-bis p. c. Embezzlement of public money, extortion, unlawful inducement to give or promise benefits, bribery and instigation to bribery of members of EU bodies and of Officials of the EU and of foreign States	1) Keeping the compulsory registers and books and the financial report to facilitate the concealment of abnormal situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes	3) Keeping the compulsory registers and books and the financial report to facilitate the concealment of abnormal situations that may be indicative, for instance, of off-balance-sheet funds set up for corruption purposes

A 4. GENERAL PRINCIPLES OF CONDUCT

In general and in order to prevent the commission of offences against the Public Administration, private-to-private corruption and instigation thereto, which are relevant to the Foundation and envisaged by the Decree, the Addressees of the Model – without prejudice to the contents of the Group Code of Conduct and of its Implementing Provisions "Conflicts of Interest" and "Fight against Corruption" and of the Procedure regarding "Transactions with Related Parties" – are

- required to:
 - abstain from such behaviours as may constitute the offences set forth in articles 24, 25 and 25-ter of Legislative Decree 231/01;
 - entertain behaviours characterised by honesty and the respect for professional ethics;
 - abstain from having relationships with the Public Administration in representation or on behalf of the Foundation, without a specific authorisation or power of attorneys, for non-professional reasons or on grounds that bear no relation to their assigned roles and functions;
 - abstain from using any privileged channels - including perfectly legal - or personal acquaintances made outside their professional sphere, with those Addressees who, by reason of their assignments, functions or mandates, interact with the Public Administration;
 - manage in a unitary manner the relations with the Public Administration for sensitive activities and to appoint an *ad-hoc* official for every dossier or multiple dossiers (if particularly repetitive) dealing with sensitive activities;
 - verify whether the stored data is accurate and consistent through automatic checks by computer systems;
 - charge only the relevant organisational unit, according to the existing operating procedures, with checking the full compliance of the contracts entered into with the Public Administration;
 - specify an explicit reason as well as document and record operations involving the use of economic or financial resources, in compliance with the principles of professional fairness and accounting soundness, so as to ensure a transparent decision-making process;
 - comply with the reporting requirements, for those authorised to incur expenses on behalf of the Foundation;
 - abstain from paying Public Administration representatives undue sums of money or granting them undue benefits of any nature, which may constitute one of the criminal offences envisaged and punished under articles 24 and 25 of Legislative Decree 231/01;
 - conduct an adequate preventive and duly documented audit of the beneficiaries of any charitable contributions or sponsorships, and make all payments only to accounts opened in the latter's name;
 - seek the relevant organisational unit's authorisation for any gifts or invitations to entertainment events extended to public officials;
 - let only the relevant organisational unit choose the partners – including employees and consultants – with whom they enter into contracts. In particular transparently; as for consultants, they must be chosen from lists of accredited consultants prepared by the relevant organisational unit; if the consultancy assignment is awarded to subjects who are not included in the above lists, the respective choice must be accompanied by an explicit reason;
 - involve the subjects in charge of judicial, tax and administrative inspections as provided below;
 - comply with the limits prescribed by the Code of Conduct for offering and accepting gifts, forms of entertainment or other benefits to or from Public Administration representatives;
 - provide the relevant Supervisor or organisational unit with information on any gifts, invitations or offers of other forms of benefits that may arouse the suspicion of undue influence in corporate decisions;
 - specify an explicit cause, document and record those operations in compliance with the principles of professional fairness and accounting soundness, so as to ensure a transparent decision-making process, in operations requiring the use of economic or financial resources;
 - perform payment operations only if formally authorised by corporate officials vested with the necessary powers;
 - verify whether payments are correct, i.e. whether they are adequately commensurate with the activity performed, also considering market conditions and the type of task to be performed;
 - in the event of charitable contributions or sponsorships, perform an adequate, duly documented, verification of the beneficiary and only make all payments to accounts opened in the latter's name;
 - inform the relevant supervisor, or directly the Surveillance Body, about any alleged or known violation that may constitute a corruption offence;

- provide promptly, correctly and in good faith all notifications, required by the law and by the regulations, to the Public Administration, by avoiding obstructing its supervisory functions in any manner; in this perspective corporate officials must:
- send the Public Administration all notifications required by the law and by regulations or sought by the Foundation for other reasons in a prompt, complete and accurate manner, by providing all data and documents prescribed or required;
- provide true, complete and correct data in the above notifications, by specifying every significant fact regarding the economic, capital, or financial position of the Foundation or of other companies of the Generali Group;
- abstain from any behaviour that may prevent the Public Administration from exercising its prerogatives (through, e.g., lack of cooperation, obstructive behaviours, reticent or incomplete answers, specious delays, concealment of significant information for the overall assessment of an operation, etc.).
- in its interactions with the Public Administration, if the Foundation is represented by a corporate subject without specific powers or delegations, the latter shall be obliged to:
 - report promptly and with full details the progress of the proceeding to his/her own supervisor;
 - report without delay to his/her supervisor, who in turn shall report to the Surveillance Body, any behaviours of the public counterparty aimed at obtaining favours, unlawful gifts of money or other benefits, including to third parties;
- the Addressees are prohibited from:
 - engaging in behaviours that, although not constituting in themselves criminal offences like those described above, may turn into such offences;
 - interacting with the Public Administration autonomously (at least two individuals must interact with Public Officials and/or with Officials in charge of Public Services);
 - being represented, in their relationships with the Public Administration, by an advisor or by another third party who is not adequately or formally authorised and, however, whenever conflicts of interest arise;
 - departing from the relevant principles and operating procedures in concluding agreements with the Public Administration;
 - making payments to encrypted or numbered bank accounts or in cash;
 - promising, offering or accepting gifts in cash or in equivalent payment instruments, as well as in marketable securities of every category either from or to Public Officials, Public Institutions or Authorities, representatives of political parties and trade unions, in general either from or to Italian or foreign public officials (including in those countries where offering gifts is common practice) or their family members, which may affect independent judgement or induce them to grant the Foundation advantages of any kind;
 - making promises of any sort (employment, stages, etc.) or granting benefits of any nature to Public Officials and/or Officials in charge of Public Services belonging to the Public Administration, to Public-Sector Authorities and/or to similar entities of the Italian State, of the European Union and of foreign countries, as well as to any other individuals or legal persons within the scope of interest of the subjects specified above;
 - rendering services to third parties which are not directly related to or fail to meet the contract provisions agreed with those subjects;
 - granting fees to suppliers of goods and services that are neither adequately justified, nor commensurate with the activity performed, also considering market conditions, the type of task in hand and current local practices;
 - providing, drawing up or handing to Public Officials and/or Officials in charge of Public Services belonging to the Public Administration, to Public Authorities and/or to similar entities of the Italian State, of the European Union and of foreign countries, declarations, data or generic documents with inaccurate, wrong, incomplete, and/or false contents in order to obtain certifications, permits, authorisations and/or licences of any kind, or to obtain funds, contributions or subsidised loans from the State;
 - conditioning in any way and with any means the freedom of self-determination of subjects who, in any capacity, are called to give testimony before Court Authorities.
 - submitting declarations, notices or documents containing false, misleading or partial information to the Public Administration, or omitting information, in order to obtain a favourable treatment from the Public Administration (e.g. to obtain concessions or authorisations, public funding);
 - paying and/or proposing the payment and/or asking third parties to propose the payment of money or the granting of other benefits to a Public official of a Court Authority, or to his/her family members, if the Foundation is a party in a legal proceeding;
 - allocating for purposes other than those for which contributions, subsidies or loans or other comparable disbursements were granted by the State, by another public authority or by the European Union;

- donating money to (senior or subordinate) representatives of other private companies in order to obtain any advantage for the Foundation;
- granting other advantages of any nature (hiring promises, use of corporate goods, etc.) to representatives of other private companies, or people close to them, who may provide any advantage to the Foundation;
- offering or accepting undue payments, as well as gifts, forms of entertainment or other undue benefits;
- granting remuneration or other advantages of any nature to external consultants that are not adequately justified or commensurate with their activities, also considering market conditions, the type of tasks to be performed and current local practices;
- donating money or granting other benefits to suppliers which are not adequately justified by the relationship established with them or which may convince them to grant an undue advantage to the Foundation;
- rendering services to third parties which are not directly related to or do not meet the contract provisions agreed with those subjects;
- departing from the principles and operating procedures adopted by the Foundation in entering agreements with third parties;
- envisaging and/or implementing waivers from standard economic and legal contract terms that are not adequately justified by normal market conditions;
- making payments on encrypted or numbered bank accounts or in cash and, in any event, to subjects other than their contract counterparties; offering undue payments.

The waivers, violations or suspected violations of the regulations governing activities at risk of crimes described in this Special Part are liable to be reported by all employees and corporate bodies according to the procedures laid down in the General Part of the Model.

A 5. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

The following paragraphs list the sensitive activities specifying, for each of them, the corporate functions involved, the relevant internal regulations (e.g. GIRS), as well as the other internal procedures (e.g. operating instructions, internal manuals).

Here are listed the sensitive activities managed, in whole or in part, by the Foundation.

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
1	Preparation and management of the budget for financing plans for the projects supported by the Foundation, as well as approval of extra-budgets	General Secretariat	- Group purchasing cycle regulation	- Implementing provisions for the fight against corruption
2	Verification of the assessment process of bodies receiving charitable contributions	General Secretariat	- Group Guideline for Community Initiatives	
3	Approval of charitable contributions	General Secretariat	- Group Guideline for Community Initiatives	
4	Monitoring of the projects funded by the Foundation	General Secretariat		
9	Managing relations with partners identified for the management of the Foundation's projects	General Secretariat		- Implementing provisions for the fight against corruption
16	Relations with representatives of the Public Administration in the context of the management of regulatory and administrative requirements, also through external subjects (e.g. notices to offices of Municipalities and Provinces, to the Revenue Office, to Tax Offices, to INPS, INAIL, filing of proxies and financial statements, filing of minutes, etc.)	General Secretariat	- Supervisory Reporting and Public disclosure Policy - Nomination, Delegated Powers and Remuneration Guideline	- Implementing provisions for the fight against corruption
17	Relations with Public Administration representatives within their inspection and control activities, their recording and acquisition of their findings (for example: Revenue Office, Guardia di Finanza, INPS, INAIL, labour inspectorate, ISPEL, SPISAL, Provincial Labour Directorate, Data Protection Authority, ISTAT, chambers of commerce, ASL, Fire Brigades, foreign authorities, etc.)	General Secretariat	- Management of relations with the Public Administration and of relevant obligations	- Implementing provisions for the fight against corruption
18	Management of the penalties imposed by administrative authorities (reception and verification of the penalties, allocation of the sums needed to cover any expenses to be incurred for the penalties).	General Secretariat		- Implementing provisions for the fight against corruption
30	Conclusion of active rental / lease contracts	General Secretariat	-	- Implementing provisions for the fight against corruption
40	Management of current accounts (opening, closing, changing specimens of signature, etc.)	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
41	Management of payments and disbursements (e.g. entering invoices, creating claims for payment)	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	

Internal

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
42	Management of petty cash	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
49	Approval of financial statements	General Secretariat	- Policy on Valuation of Assets and Liabilities other than Technical Provisions	- Implementing provisions for the fight against corruption

Internal

A 6. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to what is shown in the table in the previous paragraph, it should be emphasised that Assicurazioni Generali (the company seconding the Foundation's resources) puts in place additional control safeguards, also aiming at preventing the risk of perpetration of the offences specified in the Decree and dealt with in this Section A.

They are shown below, with direct reference to the corporate functions involved.

With regard to the sensitive activities in which the **Group Legal Affairs** function is involved, the following control safeguards have been identified:

- specific proxies have been envisaged both for the signature of the power of attorney to appear in court (based on the value of the dispute) and for any settlements of pending litigations;
- implementation of a Legal Panel, i.e. a list of lawyers selected by the Foundation and grouped by competencies and jurisdiction, to whom tasks should be assigned in case of litigations;
- segregation of duties between those who select the lawyers to be used, those who sign the power of attorneys to appear in court, those who check the correctness of invoices and those who authorise the inclusion of new lawyers in the panel, or the inclusion of a lawyer already participating in the panel in another section;
- provision of specific checks aimed at certifying that the items of invoices are correct, as compared to the contents of the engagement letter delivered to the lawyer;
- formal authorisation in compliance with existing delegations and proxies;
- constant monitoring of the progress of individual disputes and of the actual implementation of the procedural strategy shared with the appointed lawyers;
- archiving the documentation on single disputes;
regular assessment of the lawyers' performance based on specific criteria in order to assess their permanence or elimination from the panel.

With regard to the sensitive activities in which the **Corporate Tax Affairs** function is involved, the following control safeguards have been identified:

- the employees of the Corporate Tax Affairs structure perform their activities based on written proxies. When they act for other companies of the Group, they need specific written proxies authenticated by a notary public.
- in the event of extraordinary activities (e.g. enrolment and start of the assessment procedure), opinions need to be shared with the head of the Group Tax Affairs structure and with the Chief Financial Officer
- segregation of tasks between those who, within the "Tax" structure of GBS, calculate direct and indirect taxes and those who check their correctness within the Corporate Tax Affairs structure.

With regard to the sensitive activities in which the **HR BP CFO, M&A, S&BA, CM&CO, CA, Control Functions** are involved, the following control safeguards have been identified:

- archiving and formalising all the documentation (reports) generated by external companies during the assessments carried out for the stages of recruiting and promotion to executive or manager. The outcome of the assessments of candidates at various stages of the selection process is also formalised;
- Checks on hired people (e.g. collection of criminal records, check of related parties, compliance with the legislative constraints on non-EU citizens, "Fit & Proper" self-declaration).

With regard to the sensitive activities in which the **Group Treasury** function is involved, the following control safeguards have been identified:

- SAP-powered management of payments
- monitoring the balance of the individual current accounts managed by each organisation (as part of cash pooling activities) by using the Quantum environment;
- segregation of tasks of those who prepare claims for payment, those who authorise the payments and those who transmit the claims to the bank;
- segregation of tasks of those who request opening / changing a current account and those who authorise it;
- automatic lock of claims for payment, on the corporate IT system used to process those claims, if the payment recipient is different from the contract counterparty (the system, indeed, allows preparing claims for payment only by coupling them with existing invoices, which are in turn connected with a counterparty appearing in the master data or with an employee who is actually available in the master data, for the payment of salaries) or verification by hand, if it is not performed automatically by the system;

Internal

- verification of the correct authorisation of claims for payment;
- profiling users, within the corporate IT system used for managing claims for payment, which ensures that the data contained in the payment arrangements to be transmitted to banks (disabling any changes to claims for payment after their certification) are correct;
- profiling users, within the corporate IT system used for managing claims for payment, which guarantees an adequate segregation of activities (those who prepare the claims for payment cannot authorise them and those who authorise the claims for payment cannot prepare them);
- periodic monitoring of users in order to ensure that their profiles are consistent with existing delegations and proxies;
- system block for entering orders of payment for the structure's operators;
- reconciliation mechanisms for expenses;
- existence of a current account reserved for petty cash transactions;
- existence of a limited list of subjects who are authorised to withdraw money from a bank branch.

With regard to the sensitive activities in which the **Reward, Performance Management & Development** function is involved, the following control safeguards have been identified:

- preparation of a Remuneration Report and of an Annual Report for member insurance companies to be submitted to control functions and to the BoD;
- segregation of tasks: process for issuing internal measures with the involvement of other corporate functions that ensure further segmentation, also including skills outside functions (e.g. Organisation, Compliance, Risk Management, Internal Audit).

SECTION B – COMPUTER CRIMES

B 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, computer crimes and unlawful data processing, which are briefly described below and referred to in Articles 24-bis of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Offences regarding **digital documents**, as provided for in article 491-bis p. c. consist in crimes of forgery, either material or intellectual, committed on public deeds, certificates, authorisations, private deeds or private accounts, by a Public Administration representative or by a private individual, if they concern a “digital document with evidentiary effect”, i.e. an electronic document with at least a simple electronic signature.

“Digital document” means the digital representation of juridically significant deeds, facts or data (that crime extends the criminal prosecution of the offences set forth in the Book II, Title VII, Chapter III of the Penal Code to digital documents that have evidentiary effect).

The offences indicated below fall within this type of crime:

- **Intellectual forgery of certificates committed by people providing an essential public service**, as provided for in article 481 p. c., consists in the conduct of anyone who, while exercising an healthcare or legal profession, or while providing any other essential public service, falsely states, in a certificate, facts whose truth is expected to be demonstrated by that same deed;
- **Material forgery committed by private individuals**, as provided for in article 482 p. c., consists in the conduct of private individuals or Public Officials, outside the exercise of their functions, who commit one of the facts identified in articles 476 p. c. (Material forgery of official documents committed by a Public Official), 477 p. c. (Material forgery of certificates or administrative authorisations committed by a Public Official), and 478 p. c. (Material forgery of certified copies of official or private records and of certificates of the contents of documents, which is committed by a Public Official);
- **Intellectual forgery of a public record committed by a private individual**, as provided for in article 483 p. c., consists in the conduct of anyone who, in an official record, falsely states facts whose truth is supposed to be established by that same record;
- **Forgery of registers and notices**, as provided for in article 484 p. c., consists in the conduct of anyone who, while being required by law to file documents which are liable to be inspected by law enforcement authorities, or to notify those same authorities of his/her own industrial, commercial or professional activities, writes or has others write false statements;
- **Use of a forged document**, as provided for in article 489 p. c., consists in the conduct of anyone who, without participating in the forgery, makes use of a forged document;
- **Suppression, destruction and concealment of true records**, as provided for in article 490 p. c., consists in the conduct of anyone who, in whole or in part, destroys, suppresses or conceals a true public record or, in order to obtain an advantage for himself/herself or others or to cause damage to others, destroys, suppresses or conceals a holographic will, a promissory note or a credit instrument that can either be endorsed or paid to the bearer;

Unauthorised access to a computer or Internet-based system, as provided for in article 615-ter p. c., consists in the conduct of anyone who accesses illegally a computer or Internet-based system protected by security measures or who remains there against the explicit or implicit will of those who have the right to exclude him/her from it;

Unauthorised holding and disclosure of access codes to computer or Internet-based systems, as provided for in article 615-quater p. c., consists in the conduct of anyone who, in order to obtain a profit for himself/herself or others or to cause damage to others, illegally procures, reproduces, disseminates, communicates or deliver codes, keywords or other suitable means for accessing a computer or Internet-based system, which is protected by security measures, or however provide information or instructions suitable for that purpose;

Distribution of equipment, devices or computer programs aimed at damaging or disrupting a computer or Internet-based system, as provided for by article 615-quinquies p. c., consists in the conduct of anyone who, in order to unlawfully damage a computer or Internet-based system, the information, data or programs contained therein or relevant to it or in order to favour the disruption – either total or partial – or alteration of its operation, procures, produces, reproduces, imports, distributes, communicates, delivers or, however, makes equipment, devices or computer programs available to others;

Installation of equipment to intercept, prevent or interrupt IT or Internet-based communications, as provided for in article 617-quinquies p. c., consists in the conduct of anyone who, except for the cases permitted by law, installs equipment designed to intercept, prevent or interrupt the communications of a computer or Internet-based system or between multiple systems;

Damage to information, data and computer programs, as provided for in article 635-bis p. c., consists in the conduct of anyone who destroys, deteriorates, deletes, alters or suppresses information, data or computer programs owned by others, unless the fact constitutes a more serious crime;

Damage to information, data and computer programs used by the State or by another public authority, or, however, an organisation with public benefit purposes, as provided for in article 635-bis p. c., consists in the conduct of anyone who commits an offence aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs used by the State, or by another public authority, or related thereto, or, however, with public benefit purposes, unless the fact constitutes a more serious crime;

Damage to computer or Internet-based systems, as provided for in article 635-quater p. c. consists in a situation in which anyone, by behaving as described in article 635-bis p. c. or by introducing or transmitting data, information or programs, destroys, damages, renders computer or Internet-based systems owned by others totally or partially useless or seriously hinders their operation;

Damage to computer or Internet-based systems with public benefit purposes, as provided for in article 635-quinquies p. c., consists in the conduct described in article 635-quater p. c., if that conduct is aimed at destroying, damaging, rendering computer or Internet-based systems with public benefit purposes totally or partially useless, or at seriously hindering their functioning;

B 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk Self-Assessment, as available in its records, the Foundation identified sensitive activities within which some of the computer crimes or unlawful data processing offences described in article 24-bis of the Decree may be committed.

The sensitive activities identified within that Risk Self-Assessment and shown in a table containing a description of each activity, of the corporate functions involved, of the relevant offences, with *ad-hoc* examples of potential illegal behaviours. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for COMPUTER CRIMES and UNLAWFUL DATA PROCESSING
11	Management of corporate hardware systems	General Secretariat	1) Article 491-bis p. c. Digital documents 2) Article 615-ter p. c. Unauthorised access to a computer or Internet-based system 3) Article 615-quater p. c. Unauthorised holding and disclosure of access codes to computer or Internet-based systems 4) Article 615-quinquies p. c. Spreading programs aimed at damaging or disrupting a computer system 5) Article 617-bis p. c. Installation of equipment to intercept, prevent or interrupt computer-mediated or Internet-based communications 6) Article 635-bis p. c. Damage to information, data and computer programs 7) Article 635-ter p. c. Damage to information, data and computer programs used by the State or by another public entity or public benefit entity 8) Article 635-quater p. c. Damage to computer and Internet-based systems 9) Article 635-quinquies p. c. Damage to computer and Internet-based systems with public benefit purposes	1) Falsification of data entered into computer systems used by the Foundation to conduct its activities (e.g. falsification or deletion of information with evidentiary effect stored on its systems in order to eliminate the evidence of another offence or to falsify the amounts owed by or to the Foundation to / by a third party) 2) Unauthorised access to a computer or Internet-based system protected by security measures (e.g. unauthorised access to the computer system of a competitor in order to obtain information to be used for the Foundation's benefit or setting up/disclosing unauthorised user accounts to its staff, so as to allow unauthorised users to access computer systems) 3) Unauthorised dissemination, reproduction, disclosure or delivery of codes, keywords or other means for accessing a computer system of the Foundation or of third parties, which is protected by security measures, thus allowing unauthorised users to access it in order to obtain a competitive edge; 4) Distribution, reproduction, importing or provision of equipment, devices or programs capable of unlawfully damaging a computer system, the information, data or programs contained in it, or of facilitating the disruption, either total or partial, or alteration of its operation (e. g. by spreading viruses or other malignant software to competitors' systems, in order to gain a competitive edge) 5) Installation of equipment for intercepting, preventing or disrupting the communications of a computer system or between multiple systems (ad es. keyloggers, systems to obtain codes to access systems of competitors, intercept communications and obtain a business advantage) 6) Destruction, deterioration, deletion, alteration or suppression of information, data or computer programs of third parties (e.g. by tampering with data or by spreading malware or other harmful programs to gain a competitive edge) 7) Perpetration of an offence aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs used by the State, or by another public entity, or related thereto, or, however, with public benefit purposes, (e. g. destruction of data contained in the systems of police or of court offices by employees involved in judicial proceedings in order to favour the Foundation in those same proceedings) 8) Destroying, damaging or seriously hindering the operation of third-parties' computers or Internet-based systems (e.g. damaging websites of public competitors in order to cause them economic damage and a corresponding business advantage for the Foundation) 9) Perpetration of an act aimed at damaging or destroying computer or Internet-based systems used by the State, or by another public entity, or related thereto, or, however, with public benefit purposes
12	Management of corporate software systems	General Secretariat	1) Article 491-bis p. c. Digital documents 2) Article 615-ter p. c. Unauthorised access to a computer or Internet-based system 3) Article 615-quater p. c. Unauthorised holding and disclosure of access codes to computer or Internet-based systems 4) Article 615-quinquies p. c. Spreading programs aimed at damaging or disrupting a computer system	1) Falsification of data entered into computer systems used by the Foundation to perform its activities (e.g. falsification or deletion of information with evidentiary value stored on its systems, in order to eliminate the evidence of another offence or to falsify the amounts owed by or to the Foundation to / by a third party) 2) Unauthorised access to a computer or Internet-based system protected by security measures (e.g. unauthorised access to the computer system of a competitor in order to obtain information to be used for the Foundation's benefit or setting up/disclosing unauthorised user accounts to its staff, so as to allow unauthorised users to access computer systems)

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for COMPUTER CRIMES and UNLAWFUL DATA PROCESSING
			5) Article 617-bis p. c. Installation of equipment to intercept, prevent or interrupt computer-based or Internet-based communications 6) Article 635-bis p. c. Damage to information, data and computer programs 7) Article 635-ter p. c. Damage to information, data and computer programs used by the State or by another public entity or public benefit entity 8) Article 635-quater p. c. Damage to computer and Internet-based systems 9) Article 635-quinquies p. c. Damage to computer and Internet-based systems with public benefit purposes	3) Unauthorised dissemination, reproduction, disclosure or delivery of codes, keywords or other means suitable for accessing a computer system of the Foundation or of third parties which is protected by security measures, thus allowing unauthorised users to access that system in order to obtain a competitive edge; 4) Distribution, reproduction, importing or provision of equipment, devices or programs capable of unlawfully damaging a computer system, the information, data or programs contained in it, or of facilitating the disruption, either total or partial, or alteration of its operation (e. g. by spreading viruses or other malignant software to competitors' systems, in order to gain a competitive edge) 5) Installation of equipment for intercepting, preventing or disrupting the communications of a computer system or between multiple systems (ad es. keyloggers, systems to obtain codes to access systems of competitors, intercept communications and obtain a business advantage) 6) Destruction, deterioration, deletion, alteration or suppression of information, data or computer programs of third parties (e.g. by tampering with data or by spreading malware or other harmful programs to gain a competitive edge) 7) Perpetration of an offence aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs used by the State, or by another public entity, or related thereto, or, however, with public benefit purposes, (e. g. destruction of data contained in the systems of police or of court offices by employees involved in judicial proceedings in order to favour the Foundation in those same proceedings) 8) Destroying, damaging or seriously hindering the operation of third-parties' computers or Internet-based systems (e.g. damaging websites of public competitors in order to cause them economic damage and a corresponding business advantage for the Foundation) 9) Perpetration of an act aimed at damaging or destroying computer or Internet-based systems used by the State, or by another public entity, or related thereto, or, however, with public benefit purposes
13	Management of access, accounts and profiles (for instance: for management and administrative/accounting software; for Internet access and e-mail use; for the management of the credentials of system administrators, etc.)	General Secretariat	1) Article 491-bis p. c. Digital documents 2) Article 615-ter p. c. Unauthorised access to a computer or Internet-based system 3) Article 615-quater p. c. Unauthorised holding and disclosure of access codes to computer or Internet-based systems 4) Article 615-quinquies p. c. Spreading programs aimed at damaging or disrupting a computer system 5) Article 617-bis p. c. Installation of equipment to intercept, prevent or interrupt computer-mediated or Internet-based communications 6) Article 635-bis p. c. Damage to information, data and computer programs 7) Article 635-ter p. c. Damage to information, data and computer programs used by the State or by another public entity or public benefit entity	1) Falsification of data entered into computer systems used by the Foundation to perform its activities (e.g. falsification or deletion of information with evidentiary effect stored on its systems, in order to eliminate the evidence of another offence or to falsify the amounts owed by or to the Foundation to / by a third party) 2) Unauthorised access to a computer or Internet-based system protected by security measures (e.g. unauthorised access to the computer system of a competitor in order to obtain information to be used for the Foundation's benefit or setting up/delivering unauthorised user accounts to its staff, so as to allow unauthorised users to access computer systems) 3) Unauthorised dissemination, reproduction, disclosure or delivery of codes, keywords or other means suitable for accessing a computer system of the Foundation or of third parties which is protected by security measures, thus allowing unauthorised users to access that system in order to obtain a competitive edge; 4) Distribution, reproduction, importing or provision of equipment, devices or programs aimed at unlawfully damaging a computer system, the information, data or programs contained in it, or at facilitating the disruption, either total or partial, or alteration of its functioning (e. g. by spreading viruses or other malignant software to competitors' systems, in order to gain a

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for COMPUTER CRIMES and UNLAWFUL DATA PROCESSING
			8) Article 635-quater p. c. Damage to computer and Internet-based systems 9) Article 635-quinquies p. c. Damage to computer and Internet-based systems with public benefit purposes	competitive edge) 5) Installation of equipment suitable for intercepting, preventing or disrupting communications from a computer system or of between multiple systems (ad es. keyloggers, systems to obtain codes to access competitors' systems, to intercept communications and obtain a business advantage) 6) Destruction, deterioration, deletion, alteration or suppression of information, data or computer programs of third parties (e.g. through tampering with data or spread of malware or other harmful programs, in order to obtain a competitive edge) 7) Perpetration of an offence aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs used by the State, or by another public organisation, or related thereto, or, however, with public benefit purposes, (e. g. destruction of data contained in the systems of police or of court offices by employees involved in judicial proceedings in order to favour the Foundation in those very proceedings) 8) Destruction, damaging or serious hindering of the working of third-parties' computers or Internet-based systems (e.g. damage to websites of public competitors in order to cause them economic damage and a corresponding business advantage for the Foundation) 9) Perpetration of an act aimed at damaging or destroying computer or Internet-based systems used by the State, or by another public organisation, or related thereto, or, however, with public benefit purposes
14	Management and security of documents in digital formats	General Secretariat	1) Article 491-bis p. c. Digital documents 2) Article 615-quater p. c. Unauthorised holding and disclosure of access codes to computer or Internet-based systems	1) Falsification of data entered into computer systems used by the Foundation to perform its activities (e.g. falsification or deletion of information with evidentiary effect stored on its systems, in order to eliminate the evidence of another offence or to falsify the amounts owed by or to the Foundation to / by a third party) 2) Unauthorised dissemination, reproduction, disclosure or delivery of codes, keywords or other means suitable for accessing a computer system of the Foundation or of third parties which is protected by security measures, thus allowing unauthorised users to access that system in order to obtain a competitive edge;
15	Management of physical access to sites hosting IT infrastructures	General Secretariat	1) Article 491-bis p. c. Digital documents 2) Article 615-ter p. c. Unauthorised access to a computer or Internet-based system 3) Article 615-quater p. c. Unauthorised holding and disclosure of access codes to computer or Internet-based systems 4) Article 615-quinquies p. c. Spreading programs aimed at damaging or disrupting a computer system 5) Article 617-bis p. c. Installation of equipment to intercept, prevent or interrupt computer-based or Internet-based communications 6) Article 635-bis p. c. Damage to information, data and computer programs 7) Article 635-ter p. c. Damage to information, data and computer programs used by the State or by	1) Falsification of data entered into computer systems used by the Foundation to perform its activities (e.g. falsification or deletion of information with evidentiary effect stored on its systems, in order to eliminate the evidence of another offence or to falsify the amounts owed by or to the Foundation to / by a third party) 2) Unauthorised access to a computer or Internet-based system protected by security measures (e.g. unauthorised access to the computer system of a competitor in order to obtain information to be used for the Foundation's benefit or setting up/delivering unauthorised user accounts to its staff, so as to allow unauthorised users to access computer systems) 3) Unauthorised dissemination, reproduction, disclosure or delivery of codes, keywords or other means suitable for accessing a computer system of the Foundation or of third parties which is protected by security measures, thus allowing unauthorised users to access that system in order to obtain a competitive edge; 4) Distribution, reproduction, importing or provision of equipment, devices or programs aimed at unlawfully damaging a computer system, the information, data or programs contained in it, or at facilitating the disruption, either total or partial, or alteration of its functioning (e. g. by

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for COMPUTER CRIMES and UNLAWFUL DATA PROCESSING
			<p>another public entity or public benefit entity</p> <p>8) Article 635-quater p. c. Damage to computer and Internet-based systems</p> <p>9) Article 635-quinquies p. c. Damage to computer and Internet-based systems with public benefit purposes</p>	<p>spreading viruses or other malignant software to competitors' systems, in order to gain a competitive edge)</p> <p>5) Installation of equipment suitable for intercepting, preventing or disrupting communications from a computer system or of between multiple systems (ad es. keyloggers, systems to obtain codes to access competitors' systems, to intercept communications and obtain a business advantage)</p> <p>6) Destruction, deterioration, deletion, alteration or suppression of information, data or computer programs of third parties (e.g. through tampering with data or spread of malware or other harmful programs, in order to obtain a competitive edge)</p> <p>7) Perpetration of an offence aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs used by the State, or by another public organisation, or related thereto, or, however, with public benefit purposes, (e. g. destruction of data contained in the systems of police or of court offices by employees involved in judicial proceedings in order to favour the Foundation in those very proceedings)</p> <p>8) Destruction, damaging or serious hindering of the working of third-parties' computers or Internet-based systems (e.g. damage to websites of public competitors in order to cause them economic damage and a corresponding business advantage for the Foundation)</p> <p>9) Perpetration of an act aimed at damaging or destroying computer or Internet-based systems used by the State, or by another public organisation, or related thereto, or, however, with public benefit purposes</p>
26	Designation and monitoring of IT outsourcers	General Secretariat	<p>1) Article 491-bis p. c. Digital documents</p> <p>2) Article 615-ter p. c. Unauthorised access to a computer or Internet-based system</p> <p>3) Article 615-quater p. c. Unauthorised holding and disclosure of access codes to computer or Internet-based systems</p> <p>4) Article 615-quinquies p. c. Spreading programs aimed at damaging or disrupting a computer system</p> <p>5) Article 617-bis p. c. Installation of equipment to intercept, prevent or interrupt computer-based or Internet-based communications</p> <p>6) Article 635-bis p. c. Damage to information, data and computer programs</p> <p>7) Article 635-ter p. c. Damage to information, data and computer programs used by the State or by another public entity or public benefit entity</p> <p>8) Article 635-quater p. c. Damage to computer and Internet-based systems</p> <p>9) Article 635-quinquies p. c. Damage to computer and Internet-based systems with public benefit purposes</p>	<p>1) Falsification of data entered into computer systems used by the Foundation to perform its activities (e.g. falsification or deletion of information with evidentiary effect stored on its systems, in order to eliminate the evidence of another offence or to falsify the amounts owed by or to the Foundation to / by a third party)</p> <p>2) Unauthorised access to a computer or Internet-based system protected by security measures (e.g. unauthorised access to the computer system of a competitor in order to obtain information to be used for the Foundation's benefit or setting up/delivering unauthorised user accounts to its staff, so as to allow unauthorised users to access computer systems)</p> <p>3) Unauthorised dissemination, reproduction, disclosure or delivery of codes, keywords or other means suitable for accessing a computer system of the Foundation or of third parties which is protected by security measures, thus allowing unauthorised users to access that system in order to obtain a competitive edge;</p> <p>4) Distribution, reproduction, importing or provision of equipment, devices or programs aimed at unlawfully damaging a computer system, the information, data or programs contained in it, or at facilitating the disruption, either total or partial, or alteration of its functioning (e. g. by spreading viruses or other malignant software to competitors' systems, in order to gain a competitive edge)</p> <p>5) Installation of equipment suitable for intercepting, preventing or disrupting communications from a computer system or of between multiple systems (ad es. keyloggers, systems to obtain codes to access competitors' systems, to intercept communications and obtain a business advantage)</p> <p>6) Destruction, deterioration, deletion, alteration or suppression of information, data or</p>

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for COMPUTER CRIMES and UNLAWFUL DATA PROCESSING
				<p>computer programs of third parties (e.g. through tampering with data or spread of malware or other harmful programs, in order to obtain a competitive edge)</p> <p>7) Perpetration of an offence aimed at destroying, deteriorating, deleting, altering or suppressing information, data or computer programs used by the State, or by another public organisation, or related thereto, or, however, with public benefit purposes, (e. g. destruction of data contained in the systems of police or of court offices by employees involved in judicial proceedings in order to favour the Foundation in those very proceedings)</p> <p>8) Destruction, damaging or serious hindering of the working of third-parties' computers or Internet-based systems (e.g. damage to websites of public competitors in order to cause them economic damage and a corresponding business advantage for the Foundation)</p> <p>9) Perpetration of an act aimed at damaging or destroying computer or Internet-based systems used by the State, or by another public organisation, or related thereto, or, however, with public benefit purposes</p>

Internal

B 3. GENERAL PRINCIPLES OF CONDUCT

In general, and in order to prevent the perpetration of computer crimes and the illegal processing of data of significance to the Foundation, as envisaged by the Decree, the Addressees of the Model – without prejudice to the Group Code of Conduct and to its implementing provisions – are

- required to:
 - comply with the policies and procedures regarding the management of IT security, the use of information and web-based tools, of corporate networks;
 - use personal computers for work-related purposes only;
 - correctly use and store the passwords and digital signatures of the Foundation;
 - ensure the correct use of corporate IT resources by employees, who are required not to leave their own PCs unattended and/or accessible to other people and to promptly inform the heads of their offices if corporate IT equipment is lost or stolen;
 - keep confidential information and documents (e.g. personal data of employees and customers, or projects, strategies and know-how of the Foundation) with the utmost diligence and protect them adequately and continuously, according to the instructions and procedures laid down in the sectors for which they have been regulated;
 - ensure that each collaborator preserve the confidentiality of any non-public information he or she may have gained for professional reasons;
 - provide confidential information only to those who need to be familiar with it to carry out their tasks;
 - let those “in charge” use only the data that are strictly needed to perform the tasks assigned to them and for the specific goals of their function;
 - store the archives according to the security measures identified by the Foundation, with a view to limiting the access to data only to those who are explicitly authorised;
 - let all those “in charge” participate in the specific training courses on privacy and information security required by the Foundation;
 - return all assets to the Foundation at the end of their employment relationships;
- they are also prohibited from:
 - duplicating or spreading information;
 - accessing a computer or Internet-based system without possessing the required credentials or using those of other authorised colleagues;
 - unlawfully holding, procuring or disseminating access codes or, however, instruments suitable for accessing a system protected by security measures;
 - using unauthorised technical devices or software and/or suitable for preventing or disrupting the communications of a computer or internet-based system;
 - destroying, damaging, deleting, altering information, data or computer programs of third parties;
 - reproducing, distributing, or, however, providing other people with equipment, devices or programs in order to unlawfully damage a system or its respective data and programs, or favour the disruption or alteration of its operation;
 - using tools, data, computer and web-based systems so as to damage third parties, particularly by disrupting a computer system or by altering IT data or programs, also following unauthorised access, or by intercepting communications;
 - wrongfully holding or spreading code or programs capable of damaging computer systems;
 - modifying or forging digital documents of any nature or wrongfully using electronic signatures;
 - using software and/or hardware in order to intercept, falsify, alter or remove the contents of computer-based communications and/or digital documents;
 - accessing computer systems of Public Administration or of third parties without permission to obtain and/or change information for the benefit of the Foundation.

B 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

Each outsourcer, for the sensitive activities specified in paragraph B 2, defined its own relevant internal regulations (e.g. GIRS), as well as other internal procedures (e.g. operating instructions, internal manuals etc.) or further control safeguards.

SECTION C – ORGANISED CRIME AND TRANSNATIONAL OFFENCES

C 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, organised crime and transnational offences – which are described briefly below, as referred to in articles 24-ter of the Decree and 10 of Law no. 146 of 16 March 2006 – are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may be considered liable for mere attempts to commit those crimes.

Criminal organisation, as provided for in article 416 p. c., consists in the conduct of anyone who associates with three or more people to commit several crimes.

The relevant penalty is applied for the mere fact of participating in the organisation, regardless of the actual perpetration of its criminal activities.

The above-said criminal conduct can be defined as “**transnational offence**” in the cases regulated by article 3 of Law no. 146 of 16 March 2006, i.e. if the unlawful conduct:

- is committed in more than one country;
- or is committed in one country, but a substantial part of its preparation, planning, direction or control takes place in another country;
- or is committed in one country, but it involves an organised criminal group that engages in criminal activities in more than one country;
- or is committed in one country, but has substantial effects in another;

C 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

The crimes specified in article 24-ter of the Decree and in article 10 of Law 146/2006, owing to the associative character that marks most of the offences referred to in the above articles and, for the purpose of the criminal agreement, i.e. to commit any crime, may be abstractly suitable for extending the range of predicate offences (specified in Legislative Decree 231/2001) to an indefinite number of criminal acts coinciding with the possible target crimes of the organisation. The immediate consequence is that every activity conducted by the Foundation is potentially liable to the risk specified in the “231 Decree”. Recently, the Court of Cassation, however, discarded such a possibility stating that, with crimes of association, the area of potential liability of the entity in connection with the above offences is limited to those situations that are already relevant *per se*, according to the Decree.

In this context, since crimes of association may be abstractly committed by both senior and subordinate Subjects of the Foundation in agreement with individuals connected with criminal organisations or who, however, engage in unlawful activities, the Foundation identified, through a Risk Self-Assessment activity, a number of sensitive activities in which the above-mentioned offences listed in article 24-ter of the Decree and the transnational offences defined in article 10 of Law 146/2006 may be perpetrated.

The sensitive activities identified by the Risk Self-Assessment are listed below and are included in a table containing a description of each activity, of the corporate functions involved, of the relevant offences, providing specific examples of potential illegal conducts. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Examples of potential unlawful conduct for ORGANISED CRIME offences ⁷	Examples of potential unlawful conduct for TRANSNATIONAL offences ⁸
19	Search and selection of suppliers	General Secretariat	1) Being involved in an organised criminal group as well as taking part in crimes committed in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigner migrants to Italy in order to employ them illegally within the Foundation. 1) A stable association of three or more people with the goal of collaborating with external consultants with the aim of engaging in illegal conduct that brings an advantage or any form of benefit to the Foundation	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation. 1) A stable association of three or more people with the goal of hiring external consultants to engage in illegal behaviours that may bring an advantage or any form of benefit to the Foundation
21	Managing the awarding of contracts for the provision of goods and/or services (tender / direct negotiation)	General Secretariat	1) A stable association of three or more people with the goal of hiring, including through contractors / subcontractors, third-country nationals without or with expired residence permits	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation.
22	Preparation, conclusion and transmission of a contract/purchase order	General Secretariat	1) A stable association of three or more people with the goal of hiring, including through contractors / subcontractors, third-country nationals without or with expired permits	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation.
23	Designation and monitoring of suppliers	General Secretariat	1) A stable association of three or more people with the goal of hiring, including through contractors / subcontractors, third-country nationals without or with expired residence permits	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation. 1) Stable association of three or more people in order to favourably evaluate, in the selection and monitoring stages, the external consultants with whom a collaboration is in place which brings an advantage or any kind of benefits to the Foundation by engaging in unlawful conduct

⁷ The examples of illegal conducts concerning organised crime listed in the table refer to the offences defined in articles: 1) Article 416 p. c. Criminal organisation

⁸ The examples of illegal conducts concerning transnational crimes listed in the table refer to the offences defined in articles: 1) Article 3 of Law 146/2006.

ID	Description of the sensitive activity	Corporate functions involved	Examples of potential unlawful conduct for ORGANISED CRIME offences ⁷	Examples of potential unlawful conduct for TRANSNATIONAL offences ⁸
24	Receiving goods and services and authorising payments	General Secretariat	1) A stable association of three or more people with the goal of hiring, including through contractors / subcontractors, third-country nationals without or with expired residence permits	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation.
28	Preparation and transmission of purchase requests	General Secretariat	1) A stable association of three or more people with the goal of hiring, including through contractors / subcontractors, third-country nationals without or with expired residence permits	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation.
39	Management of in and out-of-court litigations (civil, criminal, administrative, labour law cases)	General Secretariat		1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example offering money to someone to convince him/her not to give testimony in a trial involving the Foundation in a different country than that in which the offence was committed.
40	Management of current accounts (opening, closing, changing specimens of signature, etc.)	General Secretariat	1) An association of three or more people that allows current account transactions to be easily carried out in order to set aside any available funds for bribery for the Foundation's benefit	
41	Management of payments and disbursements (e.g. entering invoices, creating claims for payment)	General Secretariat	1) An association of three or more people with the goal of making payments to a representative of a third-party company for corruption purposes	
42	Management of petty cash	General Secretariat	1) An association of three or more people with the goal of making payments to a representative of a third-party company for corruption purposes	
44	Administrative management of staff (e. g. processing of payroll slips, calculation of taxes and contributions, etc.)	General Secretariat	1) A stable association of three or more people with the goal of hiring, including through contractors / subcontractors, third-country nationals without or with expired residence permits	1) Being involved in an organised criminal group as well as taking part in crimes perpetrated in more than one country, or planned in one country and committed in another, or committed in one country but having effects in another, for example participating in the smuggling of foreigners to Italy in order to employ them illegally within the Foundation.

Internal

C 3. GENERAL PRINCIPLES OF CONDUCT

In general, and in order to prevent the organised crime and transnational offences that are relevant for the Foundation, as envisaged by the Decree, the Addressees of the Model, without prejudice to the Group Code of Conduct and to its implementing provisions, are

- required to:
 - confirm that any financial transaction implies previous knowledge of the – at least direct – beneficiary of the relevant sum;
 - confirm that significant tasks are assigned to natural and legal persons that have been inspected previously (including, but not limited to, consultation of Reference Lists available at the Bank of Italy, confirmation that they are included there, personal referrals, etc.);
 - confirm the commercial and professional reliability of suppliers and parties to contracts;
 - confirm that the data gathered on relationships with third parties are complete and updated, both in order to correctly and promptly identify them, and to appropriately assess their profiles;
 - confirm that payments are made correctly by checking whether the recipients / payers and the actual parties to the transactions match;
 - conducted formal and substantial inspections on the financial flows of the Foundation concerning payments to third parties and payments from intragroup operations; those inspections must consider the registered office of the counterparty, the banks used and any corporate frameworks and trust structures that are used for extraordinary transactions or operations;
 - conduct appropriate investigations on the treasury;
 - adopt adequate personnel training programmes;
 - develop indicators of anomalies so as to identify any “at risk” or “suspicious” situations based on subjective, behavioural, and location profiles of the counterparty, as well as on the economic and assets profile, characteristics and goals of the operation;
 - avail themselves of financial and banking intermediaries who are bound by transparency and fairness regulations in compliance with EU rules;
 - identify requirements that have been pre-determined by the Foundation, reviewed by it and, if necessary, regularly updated, for selecting and evaluating its counterparties;
 - verify whether the stored data is accurate and consistent through automated checks;
 - only certify in the computer payment requests from subjects holding delegated powers in line with the corporate organisation;
 - allow using computer systems for treasury management in line with the corporate organisation;
- they are also prohibited from:
 - exhibiting, collaborating in or causing behaviours that may constitute, either individually or collectively, directly or indirectly, the criminal offences referred to in article 24-ter of the Decree and in article 10 of Law no. 146 of 16 March 2006;
 - using, including occasionally, the Foundation or one of its corporate functions to allow or abet one or more organised crimes;
 - exhibiting, collaborating in or causing behaviours that, although they do not constitute a criminal offence in themselves, may potentially lead to one;
 - providing, either directly or indirectly, funds to individuals who intend to commit one or more transnational offences or who pursue, either directly or as front men, organised crime goals, including transnational, helping them achieve their criminal purposes by providing them with financial resources or, however, increasing them. For the purposes stated above, funds and financial resources are those granted to an individual or a group in the awareness – or at least with the reasonable suspicion – that:
 - they pursue organised crime goals, including transnational;
 - the intermediary receiving the funds will channel them to those groups;
 - establishing contract relationships (connected, for instance, with the purchase of goods and services) or conducting any commercial and/or financial operation, both directly and indirectly, with subjects – either natural or legal persons – whose names are included in the Reference Lists or with subjects controlled by them, when that controlling role is known. In this regard, all activities required to confirm the absence of conflicts of interest and of any suspicions of terrorism need to be carried out;
 - granting fees to third parties that are not adequately justified by the type of task to be performed and by

- current local practices;
- o receiving remuneration for non-existent deliveries or services or which lie outside the ordinary entrepreneurial activity;
- o granting charitable donations to entities and individuals included in the Reference Lists;
- o recruiting staff appearing in the Reference Lists;
- o paying fees to collaborators or external consultants that are not commensurate with the services rendered to the Foundation and inconsistent with their tasks, to be assessed based on reasonable criteria and on existing market conditions or practices.

C 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

The following table lists the sensitive activities specifying, for each of them, the corporate functions involved, the relevant internal regulations (e.g. GIRS), as well as other internal procedures (e.g. operating instructions, internal manuals).

ID	Description of the sensitive activity	Corporate functions involved	Specific control principles	
			Relevant internal regulations	Other internal procedures
40	Management of current accounts (opening, closing, changing specimens of signature, etc.)	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
41	Management of payments and disbursements (e.g. entering invoices, creating payment orders)	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
42	Management of petty cash	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	

C 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to what is shown in the table in the previous paragraph, it should be emphasised that Assicurazioni Generali (the company that seconded the Foundation's resources) puts in place additional control safeguards, also with a view to preventing the risk that the offences contained in the Decree and dealt with in this Section C might be committed.

The same are shown below with direct reference to the corporate functions involved.

The following control safeguards have been identified as to the sensitive activities involving the **HR BP CFO, M&A, S&BA, CM&CO, CA, Control Functions**:

- archiving and formalising all the documentation (reports) generated by external companies during the assessments carried out for the recruiting and promotion to executive or manager. The outcome of the assessments of candidates in the various stages of their selection process is also formalised;
- Checks on hired people (e.g. collection of criminal records, check on related parties, compliance with the legislative constraints on non-EU citizens, "Fit & Proper" self-declaration).

With regard to the sensitive activities in which the **Group Treasury** function is involved, the following control safeguards are in place:

- SAP-based management of payments
- monitoring the balance of individual current accounts managed by each organisation (as part of cash pooling activities) by using the Quantum environment;
- segregation of tasks between those who prepare claims for payment, those who authorise the payments and those who transmit the claims to the Bank;
- segregation of tasks between those who request opening / changing a current account and those who authorise it;
- automatic lock of claims for payment, on the corporate IT system used to process those claims, if the recipient of the payment is a different subject than the contract counterparty (the system allows preparing claims for payment only by coupling them with existing invoices, which are in turn connected with a counterparty appearing in the master data or with an employee who actually appears in the master data for the payment of salaries) or manual verification, if not performed automatically by the system;
- verification of the correct authorisation of claims for payment;
- profiling users, within the corporate IT system used for managing claims for payment, which ensures that the data contained in the claims to be transmitted to banks are correct (disabling any changes to claims for payment after their certification);
- profiling users, within the corporate IT system used for managing claims for payment, which guarantees an adequate segregation of activities (those who prepare the claims for payment cannot authorise them and those who authorise the claims cannot prepare them);
- regular monitoring of users to ensure that their profiles are consistent with existing delegations and proxies;
- system block for entering orders of payment for the operators of the structure;
- expense reconciliation mechanisms;
- existence of a current account reserved for petty cash transactions;
- existence of a limited list of subjects authorised to withdraw money from a bank branch.

SECTION D - CRIMES OF COUNTERFEITING OF CURRENCY, LEGAL TENDER, REVENUE STAMPS, AND DISTINCTIVE SIGNS

D 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, crimes of counterfeiting of currency, legal tender, revenue stamps, and distinctive signs, which are briefly described below and referred to in Articles 25-bis of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Spending and introducing counterfeit currency, without authorisation, in the country, as provided for in article 455 p. c., consists in the conduct of anyone who introduces in the country, buys or holds counterfeit or altered currency, with uttering purposes, or spend, or put it otherwise into circulation.

Spending of counterfeit currency received in good faith, as provided for in article 457 p. c., consists in the conduct of anyone who spends or otherwise puts into circulation (i.e. utters) counterfeit or altered currency received in good faith.

D 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through its Risk Self-Assessment activity, available in its records, the Foundation has identified sensitive activities within which some of the crimes of counterfeiting of currencies, legal tender, revenue stamps and distinctive signs set forth in article 25-bis of the Decree may be committed.

The sensitive activities identified by Risk Self-Assessment and included in a table containing a description of each activity, of the Corporate functions involved, the relevant offences, with *ad-hoc* examples of potential illegal conducts are listed below. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Examples of potential unlawful conduct for offences of COUNTERFEITING OF CURRENCY, LEGAL TENDER, REVENUE STAMPS, AND DISTINCTIVE SIGNS ⁹
42	Management of petty cash	General Secretariat	1/2) Introduction in the country or holding of counterfeit or altered currency, even if received in good faith within the management of petty cash, in order to give an unfair advantage to the Foundation or with a view to preventing adverse effects or burdens to the Foundation itself, related to acknowledging or reporting the counterfeit nature of the currency received

⁹ The examples of illegal behaviours shown in the table refer to the crimes discussed in articles 1) 455 p. c. and 2) 457 p. c.

D 3. GENERAL PRINCIPLES OF CONDUCT

In general and in order to prevent the crimes of counterfeiting of currency, legal tender, revenue stamps, and distinctive signs that are relevant for the Foundation, as envisaged by the Decree, the Addressees of the Model, without prejudice to the Group Code of Conduct and to its implementing provisions, are

- required to:
 - strictly check the valuables received and to arrange for suitable tools for confirming their authenticity;
 - pay particular attention to negotiations with counterparties who are not sufficiently well-known or negotiations involving significant amounts of money;
 - in the event of suspected counterfeit banknotes, promptly draw up a report asking for their withdrawal from circulation according to applicable laws;
 - digitally certify only claims for payment from subjects holding delegated powers in line with corporate organisation;
 - allow the use of computer systems for treasury management in line with the corporate organisation;
- are prohibited from engaging in, collaborating in or causing behaviours that may constitute, either individually or collectively, directly or indirectly, the criminal offences referred to in article 25-bis of the Decree.

D 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

The following table lists the sensitive activities specifying, for each of them, the corporate functions involved, the relevant internal regulations (e.g. GIRS), as well as other internal procedures (e.g. operating instructions, internal manuals).

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
42	Management of petty cash	Group Chief Financial Officer / Group Corporate Finance / Group treasury	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	—

D 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to what is shown in the table in the previous paragraph, it should be emphasised that Assicurazioni Generali (the company seconding the Foundation's resources) puts in place additional control safeguards with a view to preventing the risk that the offences envisaged by the Decree and dealt with in this Section D might be committed.

The same are shown below with direct reference to the corporate functions involved.

With regard to the sensitive activities in which the **Group Treasury** function is involved, the following control safeguards have been identified:

- SAP-powered management of payments
- monitoring the balance of the individual current accounts managed by each organisation (as part of cash pooling activities) by using the Quantum environment;
- segregation of tasks between those who prepare claims for payment, those who authorise the payments and those who transmit the claims to the Bank;
- segregation of tasks between those who request opening / changing a current account and those who authorise it;
- automatic lock of claims for payment, on the corporate IT system used to process them, if the recipient of the payments is different from the contract counterparty (the system, indeed, allows preparing claims for payment only by coupling them with existing invoices, which are in turn connected with a counterparty included in the master data or with an employee who is actually included in the master data for the payment of salaries) or manual verification, if not performed automatically by the system;
- verification of the correct authorisation of claims;
- profiling users, within the corporate IT system used for managing claims for payment, which ensures that the data contained in the claims for payment to be transmitted to banks are correct (disabling any changes to claims for payment after their certification);
- profiling users, within the corporate IT system used for managing claims for payment, which guarantees an adequate segregation of activities (those who prepare claims for payment cannot authorise them and those who authorise claims for payment cannot prepare them);
- periodic monitoring of users in order to ensure that their profiles are consistent with existing delegations and proxies;
- system block for entering orders for payment for the operators of the structure;
- expense reconciliation mechanisms;
- existence of a current account reserved for petty cash transactions;
- existence of a limited list of subjects authorised to withdraw money from a bank branch.

SECTION E – CORPORATE OFFENCES

E 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the corporate offences which are briefly described below and referred to in Articles 25-ter of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

False corporate accounting, as provided for in article 2621 c. c., consists in the conduct of the directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors and liquidators who, in order to achieve an unfair gain for themselves or others, in the financial statements, reports or other corporate accounts aimed at shareholders or at the public, which are required by law, knowingly state false material facts or omit relevant material facts, whose disclosure is prescribed by the law, about the economic, capital or financial position of the company or of the group to which it belongs, in such a manner as is likely to concretely mislead others. The offence also applies to any falsifications or omissions regarding assets that are owned or administered by the company on behalf of third parties.

Precluded control, as provided for in article 2625 c. c., consists in the conduct of directors who, by concealing documents or with other suitable artifices, prevent or, however, hinder the performance of control activities assigned by the law to shareholders or other corporate bodies.

Unlawful sharing of profits and reserves, as provided for in article 2627 c. c., consists in the conduct of directors who distribute profits or advance profits that were not actually gained, or allocated to reserves, under the law, or who distribute reserves, including not consisting of profits, which cannot be distributed, under the law;

Operations causing harm to creditors, as provided for in article 2629 c. c., consists in the conduct of directors who, in breach of the laws protecting creditors, decrease the share capital or perform mergers or demergers, thus causing harm to creditors.

Obstructing public supervisory authorities while exercising their functions, as provided for in article 2638 c.c., consists in the conduct of directors, general managers, executives in charge of preparing corporate accounting documents, statutory auditors and liquidators of companies or entities and other subjects which are liable to be statutorily monitored by public supervisory authorities, or bound by obligations to them, who, in their reports to the said authorities, as required by the law, present false substantive facts, despite being assessed, about the economic, capital or financial position of the supervised subjects in order to hinder those supervisory functions or, for the same purposes, conceal with other fraudulent means, in whole or in part, facts that should have been conveyed, regarding the above-said position.

The offence also applies to information concerning assets that are owned or administered by the company on behalf of third parties.

Finally, it should be noted that the Risk Self-Assessment activity has led to the detection of a high level of homogeneity between the sensitive activities considered potentially at risk of offences of private-to-private corruption and of instigating to that kind of corruption, compared to those identified as potentially relevant for the perpetration of corruption offences, in a broad and general sense, against the Public Administration. In this context, in order to draw up an Organisational Model that is as clear, effective and usable as possible for the Addressees of this Model in the mapping of the risks of perpetration of the offences specified by the Decree, the Foundation has deemed it appropriate to represent the sensitive activities considered to be at risk of corruption offences both against the Public Administration and between private parties in a unified way within this Section A. Please, refer to “Section A – Offences against the Public Administration and private-to-private corruption” for a description of the offences discussed in article 25-ter of the Decree, as specified below:

- Private-to-private corruption (article 2635 c. c.);
- Inducement to private-to-private corruption (article 2635 c. c.).

E 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk Self-Assessment, as available in its records, the Foundation identified sensitive activities in which some of the corporate crimes set forth in article 25-ter of the Decree may be committed.

The sensitive activities identified within that Risk Self-Assessment and shown in a table containing a description of each activity, of the corporate functions involved, of the relevant offences and showing *ad-hoc* examples of potential illegal conduct are listed below. Any fully outsourced sensitive activities are highlighted in grey.

Considering their specific nature of “qualified offences”, i.e. offences that can be only committed by qualified individuals (who hold a formal post within the organisation or who only perform *de facto* its functions on a continuous basis), the corporate offences referred to in this Section E always entail a direct involvement of the members of the Board of Directors of the Foundation (i.e. Chairman, Managing director, directors). Those individuals are considered subjects at risk within the sensitive processes and activities identified in the Risk Self-Assessment and listed in the tables below.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for CORPORATE crimes
34	Planning, defining and managing the meetings of the corporate bodies of the Foundation (convening, conducting the meetings of corporate bodies, managing relationships with the board of auditors, including by providing corporate documents and minutes)	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors	1) Allowing or facilitating the presentation of false material facts or omitting significant facts to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm
35	Management of the proceedings of the Board of Directors	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation of false material facts or omitting significant facts to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities
36	Managing relations with the Foundation's bodies	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors	1) Allowing or facilitating the presentation of false material facts or omitting significant facts to be reported, in such a manner as is likely to mislead others 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm
43	Preparation of reports and statements	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation of false material facts or omitting significant facts to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for CORPORATE crimes
48	Accounting and reporting of the Foundation's activities in the accounts, evaluations and budget estimates	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation, in the balance sheet, of false material facts or omitting significant information liable to be reported, in such a manner as is likely to mislead others 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities
49	Approval of the financial statements	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation, in the balance sheet, of false material facts or omitting significant information liable to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities
50	Management of activities connected with drawing up individual financial statements (information sheets, financial statement and annexes).	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation, in the balance sheet, of false material facts or omitting significant information liable to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities
51	Preparation of the financial statements	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation, in the balance sheet, of false material facts or omitting significant information liable to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for CORPORATE crimes
52	Keeping of the compulsory registers and books and of the Financial Report	General Secretariat	1) Article 2621 c. c. False accounting 2) Article 2627 c. c. Unlawful sharing of profits and reserves 3) Article 2629 c. c. Operations causing harm to creditors 4) Article 2638 c. c. Obstruction of public supervisory authorities in the exercise of their functions	1) Allowing or facilitating the presentation, in the balance sheet, of false material facts or omitting significant information liable to be reported, in such a manner as is likely to mislead others. 2) Allowing or facilitating, in the interest or for the benefit of the Foundation, the distribution of profits or advance profits that were not actually gained, or allocated to reserves under the law, or distributing reserves, including not established with profits, which cannot be distributed under the law; 3) Implementing a merger, in breach of the regulations protecting creditors, causing them harm 4) Presenting, in reports to public supervisory activities, false material facts or obstructing their monitoring activities

E 3. GENERAL PRINCIPLES OF CONDUCT

In general, and in order to prevent the corporate offences that are relevant for the Foundation, as envisaged by the Decree, the Addressees of the Model, without prejudice to the Group Code of Conduct, are

- required to:
 - abstain from committing or contributing in any way to committing the crimes referred to in articles 25-ter of the Decree, or from breaching the principles and operating procedures described in the Explanatory Document to the Organisation and Management Model;
 - engage in fair and transparent behaviours, in compliance with the laws and with operating procedures, in all activities aimed at drawing up the financial statements, the routine accounting statements and all other corporate accounts in order to provide shareholders and third parties with true and correct information on the economic, capital and financial position of the Foundation.
 - engage in a fair and transparent behaviour when dealing with related parties, in compliance with the principles of autonomy of the parties, sound management, accounting transparency and assets segregation;
 - engage in conducts aimed at ensuring the Foundation's correct operation and interaction between its corporate bodies, thus guaranteeing and facilitating every form of control on corporate management, as required by law;
 - allow members of the Board of Auditors to exercise the powers conferred on them by law; in particular, the Board and the individual auditors are allowed to perform inspections and audits at any time;
 - comply with the rules governing the correct management of relations and operations with related parties, as well as of communications and relations with Supervisory Authorities;
 - provide, with promptness, diligence and in good faith, all communications required by the law and by regulations to Supervisory Authorities, without obstructing in any way their supervisory functions; in this perspective corporate officials must:
 - send Supervisory Authorities the notifications required by law and regulations or sought from the Foundation for other reasons promptly, completely and accurately, providing all data and documents required;
 - include true, complete and correct information in the above notifications, indicating every significant fact regarding the Foundation's capital, assets or financial position;
 - abstain from any conduct that may hinder Supervisory Authorities in their activities (e.g., non-collaboration, obstructive behaviours, reticent or incomplete answers, specious delays);
 - the subjects participating in the estimation of accounting entries should comply with the principle of reasonableness and clearly specify the evaluation parameters followed, providing any supplementary information that may be needed to make sure that the document is true. The financial statements must also be complete with regard to corporate information and contain all elements required by law. The same fairness should be exercised by directors, auditors, general managers, liquidators, if any, while drawing up all other corporate documents imposed or required by law in order to ensure that they contain clear, accurate, true and complete information;
 - ensure the timely formalisation of the activities of the Foundation's bodies and the regular preparation, keeping and preservation of all the relevant corporate, accounting and tax documentation. Therefore, engaging in behaviours which, by failing to promptly update, to correctly store or by concealing documents, prevent authorities and supervisory bodies from performing their necessary supervisory activities is prohibited;
- Addressees are also prohibited from:
 - preparing or providing altered, faulty or false data on the economic, capital or financial position of the Foundation;
 - omitting to provide the data or information required by current regulations;
 - explaining the data and information used so as to provide a picture of the capital, economic, and financial position of the Foundation and of the evolution of its activities that does not correspond to their actual opinion.
 - performing activities and/or operations aimed at setting aside off-balance-sheet items (e.g. by resorting to invoices for non-existent operations or to over-invoicing), or aimed at setting aside off-balance-sheet funds or "parallel accounting", including for lower values than the criminal thresholds identified in articles 2621

- and 2622 c. c.;
- preventing or obstructing in any manner, including by concealing documents or through other tricks, the performance of the statutory control activities of the Board of Auditors;

E 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

The following table lists the sensitive activities specifying, for each of them, the corporate functions involved, the relevant internal regulations (e.g. GIRS), as well as other internal procedures (e.g. operating instructions, internal manuals).

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
34	Planning, defining and managing the meetings of the corporate bodies of the Foundation (convening, conducting the meetings of corporate bodies, managing relations with the board of auditors, including the provision of corporate documents and minutes)	General Secretariat		- Implementing provisions for the fight against corruption
35	Managing the proceedings of the Board of Directors	General Secretariat		- Implementing provisions for the fight against corruption
36	Managing relations with the Foundation's bodies	General Secretariat		- Implementing provisions for the fight against corruption
49	Approval of the financial statements	General Secretariat	- Policy on Valuation of Assets and Liabilities other than Technical Provisions	- Implementing provisions for the fight against corruption

Internal

E 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to the information contained in the table in the previous paragraph, no additional control safeguards have been found during the Risk Self-Assessment activities.

SECTION F – MANSLAUGHTER AND SERIOUS OR VERY SERIOUS INJURIES COMMITTED IN VIOLATION OF THE LAWS ON PROTECTION OF HEALTH AND SAFETY IN THE WORKPLACE

F 1. INTRODUCTION

This section adopts a partially different approach than that used to regulate other forms of risk of offence: that difference lies in the fact that that sector is characterised by the existence of a large number of regulations covering both the mechanisms for identifying duties of care, and the type and contents of precautionary safeguards. The specialty of the regulatory context, therefore, makes it necessary to build a structured prevention system, which, for its implementation, depends on the system of mandatory regulatory implementation measures already in force at the Foundation.

Typically, the crimes covered by the Decree are fraudulent, i.e. committed wilfully by the offender for that specific purpose. However, the health and safety offences in the workplace of this section of the Special Part are instead negligent, i.e. the consequence of non-compliance with laws and regulations by the offender. As a result, the exempting function of the organisational model lies in clauses aimed at convincing Addressees to adopt behaviours (unaccompanied by the intent to cause death/personal injuries) in line with the procedures prescribed by the prevention and protection system, under the regulations on the protection of health and safety in the workplace (Legislative Decree 81/08), together with the supervision requirements of the organisation model.

Since they are negligent offences, furthermore, the qualifying condition of the interest and/or advantage referred to in article 5 of Legislative Decree 231/01 does not refer to the criminal event (death or injuries) - which, by definition, was unintended – but to the violation of the accident prevention regulation caused by that conduct and, specifically, it is identified in the benefit resulting to the organisation (e.g. cost savings resulting from the failure to implement appropriate safety measures, production increase or non-interruption of production for the absence of routine and emergency maintenance operations, savings on staff training costs).

F 2. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the crimes of manslaughter and personal injuries, which are briefly described below and referred to in Articles 25-septies of the Decree, are considered applicable to the Foundation.

Manslaughter committed in breach of provisions on accident prevention and on health and safety in the workplace¹⁰, as provided for in article 589 p. c., consists in the conduct of anyone who, with negligence, causes the death of a person in violation of the provisions on occupational health and safety.

Culpable serious and very serious injuries committed in breach of provisions on accident prevention and on health and safety in the workplace, as provided for in article 590, paragraph 3, p. c., consist in the conduct of anyone who, with negligence, causes a serious or very serious personal injury in breach of the regulations on occupational health and safety.

As far as offenders are concerned, these types of offence may be committed by those who, because of their positions, carry out relevant sensitive activities, for instance:

- workers who, with their actions and/or omissions, may undermine their own and other people's health and safety;
- managers and supervisors who may also be responsible for coordinating and supervising the training and information activities;
- employers (or their delegates), as the main prevention and protection players;
- designers who, with their design and technical decisions, are responsible for complying with prevention principles in the field of health and safety at work;
- manufacturers, installers and maintenance technicians who, within their respective remits, must ensure compliance with the applicable technical standards.

¹⁰ The disciplinary system prescribes harsher penalties if the offence is committed in breach of article 55, paragraph 2 of Legislative Decree 81/08.

- principals who are responsible for the management and supervision of contract works, in accordance with the procedures laid down by the regulations.

F 3. IDENTIFICATION OF SENSITIVE ACTIVITIES

In view of the applicable regulations and of the specifications provided by the Guidelines of trade associations, it is clear that the general risk area of the company, with regard to the offences referred to in the previous paragraph, consists in any activities which involve the obligation to comply with the general and specific prescriptions on safety and hygiene in the workplace, i.e. article 2087 c. c. and Legislative Decree 81/08, as well as other relevant regulations and provisions. This is true for every corporate activity that requires the participation of workers, even a single one, according to the broad definition given by article 2 of Legislative Decree 81/08, as well as for the corporate activities entailing specific obligations and responsibilities, such as those of tenders, works contracts and contracts for the supply of utilities¹¹.

Despite the significant difficulties in linking the risk of committing crimes regarding health and safety at work to some specific functions or operational areas only and, as a result, in attributing, in general terms, to individual corporate functions / activities the risk of committing the offences considered in the Decree, a risk and control self-assessment activity, available in the Foundation's records, identified sensitive activities in which the laws and regulations on health and safety in the workplace might be disregarded.

The sensitive activities that have been identified by the risk and control self-assessment are listed below: they are shown in a table describing each activity, the functions involved, those responsible according to the relevant regulations, the offences in question, and examples of potential unlawful conduct.

¹¹ See paragraph G 8 Verification and Control Model.

ID	Sensitive activity	Corporate functions involved	Examples of potential unlawful conduct ¹²
SSL 1	Obligations under Legislative Decree 81/08 - Identification of the applicable regulatory provisions for compliance with technical/structural standards	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) ASPP (employee responsible for health and safety)	1/2) Failing to adopt and/or to comply with the prevention measures specifically prescribed by accident-prevention rules so as to achieve cost savings by failing to implement the required safety measures.
SSL 2	Obligations under Legislative Decree 81/08 - Identification of resources, roles and responsibilities to ensure workers carry out the activities aimed at implementing occupational safety procedures and instructions;	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) ASPP (employee responsible for health and safety)	1/2) Assigning tasks to subjects who do not meet the relevant technical/professional requirements compared to the functions delegated to them, so as not to employ/train suitable candidates, thus achieving cost savings.
SSL 3	Obligations under Legislative Decree 81/08 - Risk assessment and implementation of relevant prevention and protection measures	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Underestimating occupational health and safety risks and, as a result, failing to implement appropriate protection measures needed to cope with possible risks in order to gain production increases by reducing processing time.
SSL 4	Obligations under Legislative Decree 81/08 - Identification and management of collective and/or individual protection measures for containing or removing risks	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Failing to provide workers with the prescribed personal protective equipment (PPE), according to their tasks, and failing to check whether it works properly in order to contain and save costs.
SSL 5	Obligations under Legislative Decree 81/08 - Management of emergencies, of firefighting and first aid activities	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Failing to run routine checks on the application and effectiveness of emergency procedures. 1/2) Failing to provide information and training to workers about the implementation of emergency procedures to avoid investing in training programmes and to achieve cost savings.

¹² The examples of unlawful conduct listed in the table refer to the offences defined in articles: 1) Article 589 p. c. – manslaughter and 2) article 590 p. c. – negligent personal injuries.

Internal

ID	Sensitive activity	Corporate functions involved	Examples of potential unlawful conduct ¹²
SSL 6	Obligations under Legislative Decree 81/08 - Procurement management, including abroad.	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) Designated Officer (Outsourcer [GBS] – [GRE]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Awarding contracts for works, supplies and services to firms which do not meet the necessary technical-professional requirements for undertaking the assigned tasks, but which undercut the prices set by the reference market, allowing the Foundation to achieve cost savings.
SSL 7	Obligations under Legislative Decree 81/08 - Health surveillance activities	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (workers' health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Failing to submit workers to periodic medical examinations in order to cut costs, and assigning tasks entailing health hazards to workers who do not meet the necessary requirements to avoid employing or deploying further workers.
SSL 8	Obligations under Legislative Decree 81/08 - Proficiency, information, training and awareness of workers	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Failing to train workers adequately both on the prevention measures adopted by the Foundation and on the behaviours that they are required to show while carrying out their tasks in order to limit the interruptions to productive activities needed to attend their courses.
SSL 9	Obligations under Legislative Decree 81/08 - Controls over purchases, acquisition of documents and certifications prescribed by law	Employer Designated Officer (Outsourcer [GBS] – [GRE]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Introducing equipment, machinery and facilities that do not comply with the regulatory requirements or that are incompatible with work environments, in order to achieve cost savings, owing to their lower prices.
SSL 10	Obligations under Legislative Decree 81/08 - Maintenance activities aimed at complying with applicable technical, health and safety standards	Employer Designated Officer (Outsourcer [GBS] – [GRE]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Neglecting the maintenance of equipment, machinery and facilities used by workers in carrying out their tasks to achieve cost savings.
SSL 11	Obligations under Legislative Decree 81/08 - Reporting, participation and consultation, management of regular meetings on safety, consultation of the workers' representatives on safety	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Underestimating or underrating hazards to health and safety in the workplace owing to, e.g., lack of communication or involvement of workers or their representatives, in order to limit the business interruptions needed to involve workers or their representatives.

Internal

ID	Sensitive activity	Corporate functions involved	Examples of potential unlawful conduct ¹²
SSL 12	Obligations under Legislative Decree 81/08 - Management of documents and logging systems in order to ensure that activities are traceable	Employer Designated Officer (Group Chief HR & Organisation Officer [Assicurazioni Generali]) RSPP (health and safety officer) (Prevention of risks and safety in the workplace [GBS]) Occupational Health Physician (Prevention of risks and safety in the workplace [GBS]) RLS (workers' health and safety officer) ASPP (employee responsible for health and safety)	1/2) Failing to prepare documents supporting prescribed activities and to file them in order to contain processing time.

F 4. GENERAL PRINCIPLES OF CONDUCT

The Model is not intended to replace the law prerogatives and responsibilities that bind the subjects identified by Legislative Decree 81/08 and by further applicable regulations. Instead, it is a further control measure confirming the existence, effectiveness and adequacy of the structure and organisation implemented in compliance with the special regulations in force on accident prevention, and the protection of health and safety at work.

In general and in order to prevent occupational accidents and diseases, the Addressees of the Model, as well as all the subjects identified by the health and safety legislation who have duties of care towards third parties (e.g. occupational health physicians, designers, suppliers), in conducting operations within the sensitive activities listed in the previous paragraph, without prejudice to the Group Code of Conduct, in operating procedures and in accident prevention regulations, are required to:

- comply with regulations and with internal corporate procedures for collective and personal protection, in particular providing every appropriate check and taking suitable steps to safeguard the health and safety of external collaborators and/or people who may be present in the workplace;
- effectively use work equipment, as well as safety devices;
- effectively use the protection devices made available;
- immediately report to those responsible (in view of their responsibilities) any faults to the above devices, as well as any hazards they may become aware of;
- directly intervene to address a danger, only in urgent cases, in keeping with their responsibilities and possibilities;
- undergo any prescribed health inspections;
- attend prescribed training courses;
- contribute to meet all obligations set by the relevant authority or, at any rate, needed to protect the workers' safety and health at work.

They are also prohibited from:

- engaging in, collaborating or causing behaviours that, taken individually or collectively, may constitute, either directly or indirectly, the crimes referred to in this section;
- removing or changing without permission safety, alarm or control devices;
- engaging in careless behaviours as to the safeguard of their own health or safety, in keeping with their training and experience, as well as with the instructions and means provided or prepared by their employers;
- conducting, on their own initiative, operations or manoeuvres that they are not supposed to perform or that may jeopardise their own safety or that of other workers.

In general, with reference to the above behaviours, the corporate officials in charge of implementing safety measures - each one for the activities (s)he is responsible for - ensure:

- a) compliance with legal technical-structural standards connected with equipment, plants, workplaces;
- b) the implementation of risk assessment activities and the preparation of the resulting prevention and protection measures;
- c) the implementation of organisational changes aimed at coping with emergencies, providing first aid, managing procurement;
- d) that periodic meetings on safety and consultations with the Workers' Health and Safety Representatives are held properly;
- e) health surveillance activities;
- f) staff training and information activities, according to a plan laid down in compliance with the regulations in force from time to time;
- g) supervision activities with regard to the staff's compliance with occupational safety procedures and instructions;
- h) acquisition of the documents and certifications required by law;
- i) periodic checks on the application and effectiveness of the adopted procedures.

In order to implement a consistent system for managing safety at work, which encompasses working techniques, organisation and conditions, social relationships and the influence of workplace factors, the Foundation develops:

- suitable systems for recording the performance of the activities referred to in the previous sub-items a) to i);
- a structure of functions ensuring the technical skills and the powers needed to verify, assess, manage and control risks, as well as a disciplinary system suitable for punishing any failure to adhere to the measures specified in the model, according to the regulations in force;
- a suitable system for checking the implementation of the set goals on safety and of the model itself and for ensuring that the measures taken remain suitable over time. The review and any changes to the organisational model must be adopted when significant breaches of the rules on accident prevention and on occupational health are discovered or when changes in the organisation and in its activities following new scientific and technological developments occur.

Internal

F 5. THE ORGANISATIONAL STRUCTURE REGARDING HEALTH AND SAFETY AT WORK

The Foundation is endowed with organisational tools (corporate charts, documents describing roles and responsibilities, procedures, etc.) which are based on general principles: familiarity within the Foundation, definition of roles, clarity and completeness in the description of the responsibilities and powers of each function, accurately defined lines of reporting.

In keeping with the Foundation's organisational and functional scheme and in compliance with regulatory requirements, the tasks and responsibilities on health and safety at work have been identified and defined, from the Employer to the Workers, according to the regulations in force.

This structure includes, in particular, the following subjects:

- **Employer:** the subject identified by the Foundation's Board of Directors who is vested with the powers envisaged by article 2 of Legislative Decree 81/08. The employer, with most appropriate methods for his/her purposes, monitors systematically the delegated functions, also by gathering information from the Prevention and Protection Service Manager, the Occupational Health Physician, the Workers' Health and Safety Representative or from any worker with responsibilities in the field of health and safety at work within the Foundation;
- **Employer's Designated Officer:** executive vested with the complex organisational powers envisaged by article 16 of Legislative Decree 81/08.

The Employer, also in order to meet the obligations of Legislative Decree 81/08, avails himself/herself of the technical/organisational support of external subjects appointed through *ad-hoc* agreements and by assigning appropriate powers to Generali Group companies (e.g. Generali Business Solutions S.C.p.A. e Generali Real Estate S.g.r.).

As for the management of the health and safety of the Foundation's workers, within the Generali Group a specific function is identified – within Generali Business Solutions S.C.p.A. – with the responsibility of providing indications and collaborating with the various employers of contractor companies in order to fully implement, according to homogeneous criteria within the Group, the rules contained in the TUS and/or the relevant local regulations in force in the various countries in which Generali operates.

F 6. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

For each of the sensitive activities referred to in paragraph F 3., the control principles defined to protect against the risk of committing the aforementioned crimes are reported below. The said control principles are or may be laid down by relevant internal regulations (e.g. GIRS, Guidelines) or by other internal procedures (e.g. operating instructions, internal manuals).

ID	Sensitive activity	Specific principles of control	
		Relevant internal regulations	Other documents/relevant procedures
SSL 1	Obligations under Legislative Decree 81/08 - Identification of the applicable regulatory provisions for complying with technical/structural standards	—	<p>- Compliance with the current relevant rules (laws, technical standards and regulations, etc.) is ensured by keeping specific records that monitor:</p> <ul style="list-style-type: none"> • identification of and access to specific regulations applicable to the organisation; • updating to new laws; • periodic checks about compliance with applicable regulations.
SSL 2	Obligations under Legislative Decree 81/08 - Identification of the resources, roles and responsibilities to ensure that workers follow the procedures and instructions for occupational safety;	- Operating Procedure on the Protection of Health and Safety at Work	<p>- The organisational structure, in line with regulatory provisions, consists in:</p> <ul style="list-style-type: none"> • the deed whereby the Employer is identified by the Board of Directors; • Commissions and Proxies; • Appointments; • Organisational charts. <p>- For all the individuals identified for the management of health and safety in the workplace, suitable technical and professional requirements are laid down which may also originate from specific regulatory provisions; those requirements, which must be maintained over time, must be met by the subject prior to being vested with his/her tasks and may also be achieved through specific training courses. In general, for instance:</p> <ul style="list-style-type: none"> • management, coordination and control responsibilities are formalised within the Foundation; • the subjects required by the regulations on occupational health and safety have been duly appointed and the powers they need to serve their roles have been properly conferred upon them; • the system of proxies, powers of signature and powers of expenditure is built consistently with the responsibilities assigned; • the assignment and exercise of powers within a decision-making process is consistent with the positions of responsibility and with the significance and/or criticality of the underlying hazard situations; • those who take or implement the decisions and those who are responsible for performing the checks required by law and by the control system procedures are not the same subjects; • the subjects responsible and/or appointed according to the current regulations on hygiene and safety in the workplace possess adequate and effective skills in the field. <p>- If some of the responsibilities need to be transferred, this can be done by delegating functions. In compliance with Article 16 of Legislative Decree 81/2008, this occurs on a specified date, in writing, by defining exhaustively the characteristics and limits of the responsibility and its spending power.</p>

Internal

ID	Sensitive activity	Specific principles of control	
		Relevant internal regulations	Other documents/relevant procedures
SSL 3	Obligations under Legislative Decree 81/08 - Risk assessment and implementation of relevant prevention and protection measures	—	<p>- The task of drawing up the Risk Assessment Document cannot be delegated by the Employer, who, to that end, is supported by other individuals, such as the head of the prevention and protection service, the occupational health physician, and the Workers' Health and Safety Representative. The Risk Assessment must be based on criteria defined in advance, in compliance with Articles 15, 17, and 28 of Legislative Decree 81/2008. Those additional criteria concern, amongst others, the following aspects:</p> <ul style="list-style-type: none"> • routine and non-routine activities; • the activities of all those who have access to the workplace (including external workers); • human behaviour; • external hazards; • dangers posed by processing or by the surrounding environment; • infrastructures, equipment and materials available in the workplace; • changes, including temporary, made to processes and their impact on operations, processes and activities; • any legal obligations applying to risk assessment and to the implementation of the necessary control measures; • design of working environments, machinery and equipment; • operating and working procedures. <p>- All data and information needed to assess risks and, as a result, to identify protection measures (e. g. technical documentation, instrumental measures, outcomes of internal surveys) should be clear, complete and truly represent the Foundation's situation.</p> <p>- The RAD must bear a certified date.</p>
SSL 4	Obligations under Legislative Decree 81/08 - Identification and management of collective and/or individual protection measures to contain or eliminate risks	—	<p>- The tool of risk assessment helps identify the necessary safeguards, both personal and collective, protecting workers; in particular, the following aspects are regulated:</p> <ul style="list-style-type: none"> • identification of the activities requiring PPE to be used; • definition of the criteria for choosing PPE, which must ensure that the PPE itself is adequate for the kinds of risk identified in the assessment phase and its compliance with current technical standards (e.g. EC marking); • establishing the methods for delivering and, where necessary, for preserving the PPE; • establishing a schedule to ensure compliance with protection requirements.

Internal

ID	Sensitive activity	Specific principles of control	
		Relevant internal regulations	Other documents/relevant procedures
SSL 5	Obligations under Legislative Decree 81/08 - Management of emergencies, of firefighting and first aid activities	- Operating Procedure on the Protection of Health and Safety at Work	<p>- Emergency management is implemented by the emergency planners' structure, who put in place specific plans for all locations where the Foundation conducts its business and that include:</p> <ul style="list-style-type: none"> • identification of any situations that may cause a potential emergency; • definition of methods for responding to emergencies and preventing or mitigating their negative consequences on health and safety; • updating of emergency procedures in the event of accidents or negative outcomes of periodic simulations <p>- The plans specify the escape routes and the methods the staff is required to adopt to implement emergency reporting and management measures.</p> <p>-The staff includes the emergency response workers: they are sufficient in number and have been trained according to legal requirements.</p> <p>- Suitable firefighting systems, which were chosen by type and number based on the specific fire risk assessment or on the indications of the relevant authorities are available and kept in good working order; suitable medical equipment is also available and properly maintained.</p> <p>- The effectiveness of emergency measures is guaranteed by regular tests, so as to ensure that the staff is fully aware of the correct behaviours and use the suitable recording tools for providing evidence of the outcomes of those test, inspection and maintenance activities for the safeguards in place.</p>
SSL 6	Obligations under Legislative Decree 81/08 - Procurement management, including abroad.	- Operating Procedure on the Protection of Health and Safety at Work	<p>- The individuals performing work must meet appropriate technical-professional requirements, as certified by their enrolment in the chambers of commerce (CCIAA). They must comply with insurance and social security obligations towards their staff, also by submitting the certificate of social security compliance (DURC).</p> <p>- The contractor company, in the cases covered by the law, must issue the declaration of conformity to the state of the art at the end of its work.</p> <p>- With regard, in particular, to suppliers, installers and external maintenance technicians of machinery, plants and any type of safety tools and working equipment to be implemented or installed inside areas under the legal responsibility of the Foundation's employer, specific control safeguards have been implemented, which include:</p> <ul style="list-style-type: none"> • verification procedures for suppliers which also include their own and their employees' compliance with safety procedures; • definition of the scope of intervention and of its impact in a written contract specifying the safety costs; • definition of the access and activities carried out on site by third parties, with a specific evaluation of the interfering risks linked to their presence and drawing up the coordination documentation required (e.g. DUVRI- PSC), signed by all involved external subjects and promptly adjusted, if the preconditions for interventions change; • contract clauses concerning any non-compliance by third-parties' workers at corporate sites with safety measures, which require appropriate alarms to be activated and penalties imposed; • systems for detecting the presence of third-party workers at the corporate site; • formalisation and traceability by managers and employers of compliance with the control safeguards listed so far.

Internal

ID	Sensitive activity	Specific principles of control	
		Relevant internal regulations	Other documents/relevant procedures
SSL 7	Obligations under Legislative Decree 81/08 - Health surveillance activities	- Operating Procedure on the Protection of Health and Safety at Work	- Prior to assigning any task to workers, their requirements need to be verified both with regard to their technical aspects (see the following sensitive activity: proficiency, information, training and awareness of workers), and with regard to any healthcare data found during risk assessment. - The fitness test is performed by the occupational health physician who, based on the results of the risk assessment, formulated the health surveillance protocol, which contains the types of tests workers need to undergo in connection with the risk peer group to which they belong. - After the test, the occupational health physician issues an assessment as to the total or partial medical fitness or unfitness for the task.
SSL 8	Obligations under Legislative Decree 81/08 - Proficiency, information, training and awareness of workers	- Operating Procedure on the Protection of Health and Safety at Work	- All staff receives appropriate information about the correct methods for fulfilling their tasks, is trained and, in the cases covered by the regulations, is coached. A documentation of that training and/or coaching is required. Training activities are in various ways (e.g. classroom training, written reports) as defined by the Foundation and envisaged in current regulations. - The choice of trainers may be tied to specific regulatory provisions. - Information, training and coaching activities are documented: the documentation on staff training is stored and is also used to assign new tasks. - The training activity is conducted so as to: <ul style="list-style-type: none"> • ensure, also through appropriate planning, that any individual under the organisation's control is proficient, based on adequate education, training or experience; • identify the training needs connected with the activities carried out and to provide training or consider other actions to meet those needs; • ensure that the staff is aware of the actual or potential impact of their work, of the correct behaviours to be adopted and of its roles and responsibilities. - The effectiveness of training activities or of any other actions conducted is verified and the relevant records are kept.
SSL 9	Obligations under Legislative Decree 81/08 - Controls over purchases, acquisition of documents and law-mandated certifications	—	- The purchase of equipment, machinery and facilities is conducted after assessing their health and safety requirements, while also taking into account the workers' opinions, as voiced by their representatives. The equipment, machinery and facilities must be compliant with current regulations (e.g. EC marking, declaration of conformity issued by the installer). If applicable, according to the relevant legal provisions, their commissioning shall be subject to initial test or type approval procedures. - Prior to the use of new equipment, machinery or facilities, the worker in charge must be appropriately trained and/or coached. - Purchasing activities are conducted in order to: <ul style="list-style-type: none"> • establish the criteria and methods for qualifying and checking the suppliers' requirements; • define the methods for checking the compliance of equipment, facilities and machinery to be purchased with current regulations (e.g. EC marking), as well as the criteria and methods for assessing acceptability requirements; • provide, if applicable, for methods for performing inspections at the acceptance, initial tests and type approval stages. - If services are purchased, including intellectual services (e.g. design services to be rendered to the company or to possible customers), the company subjects the designation activity to the preliminary verification of the competencies of its suppliers, also based on past experiences and any mandatory requirements (e.g. membership of professional associations). The Foundation inspects their work according to its own internal procedures. If the activities undertaken by those subjects may affect the exposure to risks for the health and safety of its workers, the Foundation activates in advance, amongst others, the prevention and control measures specified in article 26 of Legislative Decree 81/08.

Internal

ID	Sensitive activity	Specific principles of control	
		Relevant internal regulations	Other documents/relevant procedures
SSL 10	Obligations under Legislative Decree 81/08 - Maintenance activities aimed at complying with applicable technical, health and safety standards	—	<ul style="list-style-type: none"> - All equipment, machinery and facilities that may significantly affect health and safety are subject to routine maintenance protocols with timing and methods that may also be set by manufacturers. Any specialist interventions are carried out by subjects who meet mandatory requirements, who are also there to provide the necessary documents. - Maintenance activities on safety devices should be recorded. - Maintenance activities are conducted so as to: <ul style="list-style-type: none"> • establish the methods, timing and responsibilities for scheduling and performing routine maintenance and inspections, where envisaged, of equipment, facilities and machinery and regular checks on their efficiency; • define the methods for recording maintenance operations and the relevant responsibilities; • define the methods for reporting anomalies, identify the most suitable tools for disseminating those methods, identify the functions required to start the respective maintenance process (non-routine maintenance).
SSL 11	Obligations under Legislative Decree 81/08 - Reporting activities, participation and consultation, management of regular meetings on safety, consultation of the workers' safety representatives	—	<ul style="list-style-type: none"> - Reporting must: <ul style="list-style-type: none"> • concern the authorisation powers, hierarchical lines of reporting, and procedures; • be widespread, effective, authoritative, clear and detailed, periodically repeated. - The staff is involved and consulted by means of: <ul style="list-style-type: none"> • internal communication between the various levels and functions of the organisation; • communication with suppliers and other visitors in the workplace; • receiving and answering messages from the external parties involved; • workers' participation, including via their representatives, through: i) their involvement in identifying hazards, assessment of risks and development of protection measures; ii) their involvement in the investigations on an accident; iii) their consultation whenever there are changes that may significantly affect health and safety conditions. - The Employer and the PPSM, with the OHP's and the WSPs' collaboration, hold meetings, at least once a year, which discuss the issues of risk prevention and protection. The meetings are adequately formalised through <i>ad-hoc</i> minutes.
SSL 12	Obligations under Legislative Decree 81/08 - Management of documents and recording systems to ensure traceability of activities	—	<ul style="list-style-type: none"> - The management of documentation is a prerequisite for maintaining the organisation, management and control model; by properly managing the documentation and by adopting appropriate recording systems, the goal of providing evidence of the concrete results obtained is achieved, also ensuring that the decision-making procedures are traceable. The availability and updating of the documentation, originating both inside and outside, is guaranteed (e.g. documents on products and substances). - Any accidents at work that entail an absence of at least one day, are promptly, accurately and chronologically entered in a special register. Furthermore, appropriate internal procedures for outlining the methods and terms for acquiring and transmitting data regarding accidents at work are adopted, furthermore, a system of information flows is implemented to allow information to circulate within the company in order both to favour the involvement and awareness of all Addressees – within the limits of their roles, functions and responsibilities – and to ensure that any evidence of shortcomings or violations of the Model is promptly and adequately provided, and that the actions needed for its update are undertaken; - Both internal and external documents and records – the latter being special documents – are managed, ensuring that they are available, traceable and correctly kept.

Internal

F 7. FURTHER CONTROL SAFEGUARDS

Pursuant to article 18, paragraph 3-bis of Legislative Decree 81/08, on the supervision duties of employers and managers about compliance with occupational safety obligations by supervisors, workers, designers, manufacturers and suppliers, installers and occupational health physicians, specific safeguards are envisaged.

They are shown below, with immediate reference to the corporate functions involved.

With reference, in particular, to the **supervisors'** obligations (article 19 of Legislative Decree 81/08), specific control measures are envisaged, which require employers or their delegates to:

- schedule and conduct random checks on the actual training received by the subjects who access areas exposing them to specific serious hazards;
- schedule and conduct random checks on any reports of anomalies sent by supervisors, as well as those regarding the conduct of supervisors themselves;
- conduct checks on supervisors' reports about anomalies of work instruments and equipment and of personal protective equipment, and about other dangerous situations, by checking the actions undertaken by the safety officers in charge and any follow-ups to those actions.
- conduct checks as to whether supervisors have actually attended the internal training courses prepared for them.

With particular reference to the supervision of **workers'** obligations (article 20 of Legislative Decree 81/08), specific control measures are envisaged, requiring employers or their delegates to:

- schedule and conduct random checks on the actual training received by workers who access areas exposing them to a serious and specific hazard;
- schedule and conduct random checks on reports of anomalies by supervisors;
- conduct checks about whether workers have actually attended the internal training courses set up for them.
- check whether workers have actually undergone the medical checks required by law or provided by the occupational health physicians.

With regard, in particular, to the supervision of external workers, the Foundation implements the control safeguards envisaged for the compulsory supervision of designers and for checking manufacturing and installation.

As for the obligations of **designers, manufacturers, suppliers, installers and maintenance technicians of machinery, facilities and any kind of safety device and work equipment** (articles 22, 23, 24 and 26 of Legislative Decree 81/08), specific control measures are envisaged, requiring that:

- the scope of intervention and of its impact be clearly defined within a written contract;
- access and activities on site conducted by third parties be defined, with a specific evaluation of the interfering risks related to their presence and the preparation of the DUVRI document, which is to be signed by all involved external subjects and promptly amended, should the preconditions for intervening change;
- upon delivery of machinery, facilities and any kind of safety devices, the presence of EC markings, service booklets, certificates of conformity, and – if required – type approval requirements, as well as whether the specifications of the product are those expected, should be confirmed.
- contract clauses be included, concerning any non-compliance with safety measures by third-parties' employees at corporate sites, i.e. the activation of appropriate alarms and the penalties to be imposed;
- verification procedures for suppliers should also consider their own and their employees' compliance with safety procedures;
- systems be introduced for detecting the presence of third-party workers at corporate sites and for checking compliance with corporate safety principles, as possibly enshrined in contracts;
- executives and employers formalise and trace their monitoring of compliance with the control safeguards listed so far;
- within interventions affecting buildings, any documentary evidence kept at relevant entities (fire departments, local health authorities, etc.) be updated, as required by current regulations.

With particular reference to the obligations of **occupational health physicians** (article 25 of Legislative Decree 81/2008), specific control measures are envisaged, which require employers or their delegates to:

- verify whether occupational health physicians are qualified and meet the legal requirements for performing their functions;
- confirm that occupational health physicians regularly participate in coordination meetings with the HPPS, the workers' safety representatives, and the Employers themselves, in which occupational safety themes are debated, including those relating to corporate risk assessments and those affecting corporate social responsibility;
- check that occupational health physicians continuously and correctly implement the healthcare protocols and corporate procedures on health surveillance.

Internal

Finally, specific checks are put in place in order for the organisational system of the Foundation, which was set up according to the applicable regulations on safety in the workplace and of accident prevention, to be constantly monitored and given the best possible chances to operate.

In order to confirm that the provisions of Legislative Decree 81/08 and the special regulations in force on accident prevention, protection of health and safety at work are actually implemented, the following is required:

- such subjects as employers, the Heads of the Prevention and Protection Service (HPPS) and the occupational health physicians (OHP) must regularly update the Surveillance Body (SB) of the Foundation about safety in the workplace;
- the HPPS and the OHP must promptly notify any deficiencies, anomalies and non-compliance they may have found;
- the HPPS must participate in periodic meetings with the Foundation's SB in order to illustrate the most significant changes that have been made to the Risk Assessment Document (RAD) and to the safety management system procedures;
- the staff, the workers' safety representative (WSP), the OHP, the HPPS and the Employer may provide the SB with information about any deficiencies in the protection of health and safety in the workplace;
- employers must ensure that all subjects required by the sector's regulations are appointed and are provided with adequate, clear and sufficiently specific delegated powers and possess the required skills and characteristics, as well as any powers (including spending powers) which are adequate to the task in hand, and that the functions and powers delegated to them are actually exercised;
- the SB, in exercising its functions, may require the assistance of the safety officers appointed by the Foundation, as well as of competent external consultants.

F 8. THE VERIFICATION AND CONTROL MODEL

The adoption of an organisational, management and control model maintains a decisive function exempting the organisation from its liability. For these types of offence, in preparing this Model, the provisions of article 30 of Legislative Decree 81/08 have been considered. It provides exempting function to organisational models that are oriented to fulfilling specific juridical obligations, providing accurate indications for assessing the suitability of the model itself.

Legislative Decree 81/2008 indeed established a basic minimum content for the above-mentioned organisational model on this matter. Its article 30 provides that:

"The organisation and management model suitable for exempting legal persons, companies and associations – including without legal personality – as referred to in the Legislative Decree no. 231 of 8 June 2001, from any administrative liability must be adopted and effectively implemented, ensuring a corporate system for complying with all legal requirements concerning:

- a) respect for legal technical-structural standards related to equipment, facilities, workplaces, chemical, physical and biological agents;
- b) risk assessment and setting up of the resulting prevention and protection measures;
- c) organisational activities, such as emergencies, first aid, procurement management, regular meetings on safety, consultations with the workers' safety representatives;
- d) health surveillance activities;
- e) information and training activities for workers;
- f) supervisory activities with regard to compliance by workers with occupational safety procedures and instructions;
- g) acquisition of documents and certifications required by law;
- h) regular checks on the application and effectiveness of the adopted procedures.
- i) The organisation and management model referred to in paragraph 1 must include suitable systems for recording the activities described in paragraph 1.
- j) The organisational model must in any case include, as required by the nature and size of the organisation and by the type of activity, a number of functions that ensure the technical skills and powers needed to verify, assess, manage and control risks, as well as a disciplinary system suitable for punishing any failure to adhere to the measures specified in the model.
- k) The organisational model must also include a suitable control system for implementing the same model and for maintaining the suitability conditions of the adopted measures over time. The review and any changes to the organisation model must be adopted whenever significant breaches of the rules on accident prevention and occupational health are discovered or when changes in the organisation and in its activities as a result of scientific and technological advancement occur.

The regulation, as a result, prescribes that – by the legislator’s express will – the activities specifically referred to in that article must be considered sensitive and protected, regardless of any assessment, conducted in the risk self-assessment stage, about the concrete possibility that crimes might be committed.

That said, the Foundation adopts the “Verification and Control Model” described hereunder, which includes the rules listed in the following items from a) to i), as well as a list (intended as a non-exhaustive example) of violations of rules concerning health and safety in the working place.

Having already stated in paragraph G 5. that the Foundation’s Board of Directors identified, according to article 2 of Legislative Decree 81/08, an employer and that the latter has in turn delegated certain functions to other subjects, the expected requirements are as follows:

- a) the delegates of functions send regularly, at least on an annual basis, the Employer and the Surveillance Body (hereinafter also shortened into “SB”) a written report on the fulfilment of all judicial obligations referred to in article 30, paragraph 1, of Legislative Decree 81/08 and on all issues that have emerged on health and safety at work within their competence, as well as about the corrective measures taken;
- b) The Employer, using the most fit-for-purpose methods, monitors systematically the exercise of delegated functions, possibly gathering information from the Prevention and Protection Service Manager, the Occupational Health Physician, the Workers’ Health and Safety Representative or from any worker with responsibilities in the field of health and safety at work within the Foundation;
- c) The Employer conducts regular, at least annual, verifications, checks and simulations of firefighting, first aid or emergency operations;
- d) The Employer sends the Board of Directors and the Surveillance Body a written report, at least on an annual basis, concerning the fulfilment of all legal obligations on health and safety at work as per article 30, paragraph 1 of Legislative Decree 81/08, on the verifications conducted regarding the appropriate performance of delegated activities, on the checks and simulations of firefighting, first aid, or emergency operations, on the issues found and on the measures taken by him/herself and/or by the functions’ delegates, on organisational changes and on any accidents that may have occurred over the year, which were so significant as to affect the functionality of the Verification and Control Model;
- e) the Employer notifies in writing the Surveillance Body as well as the Board of Directors about every significant violation of the rules contained in the Verification and Control Model, as well as every change in the organisation or in accident-prone activities, in order to review and amend the Model itself;
- f) the Employer, should (s)he gain knowledge (either directly or from someone else) of serious and/or repeated violations committed by delegates in the exercise of their delegated functions either has them immediately replaced, if a serious and impending risk of accident exists, or applies to the same individuals the disciplinary measures set forth in the relevant section of the General Part of this Organisation and Management Model, according to the severity of the violation, its possible repetition or its consequences. The punished violations include, but are not limited to, the following, where applicable:
 - failure to designate the Risk Prevention and Protection Manager.
 - failure to appoint the Occupational Health Physician;
 - failure to prepare the Risk Assessment Document required by article 26, paragraph 3 of Legislative Decree 81/08 or failure to deliver a copy thereof to the Workers’ Health and Safety Representatives, if they so request;
 - failure to designate in advance the workers tasked with implementing fire prevention and firefighting measures, evacuation from workplaces in the event of serious and immediate hazards, rescue operations, first aid and, however, emergency management;
 - failure to consider, in assigning tasks to workers, their skills and conditions with connection with their health and safety;
 - failure to provide workers with the necessary, suitable personal protective equipment, after hearing the Prevention and Protection Service Manager and the Occupational Health Physician;
 - failure to take the appropriate measures to ensure that only the workers who have received adequate, specific training may access areas that expose them to specific serious risks;
 - failure to ask single workers to comply with the current regulations, as well as with the corporate provisions on health and safety at work and on the use of collective and personal protective equipment handed out to them;
 - failure to ask the Occupational Health Physician to fulfil the requirements set forth in Legislative Decree 81/08;
 - failure to take the measures to control hazardous situations in case of emergency and failure to disseminate the instructions so that workers, in the face of a serious, immediate and inevitable danger, leave their workplace or the danger zone;
 - failure to inform, as quickly as possible, workers exposed to a serious and immediate danger about the

- danger itself and the protection measures taken or to be taken;
- failure to meet the information, training and coaching obligations referred to in articles 36 and 37 of Legislative Decree 81/08;
 - failure to abstain – except in justified cases where health protection and safety are called for – from asking workers to resume their activities in work situations posing serious and immediate dangers;
 - preventing workers, specifically their Health and Safety Representative, from checking the implementation of safety and health protection measures;
 - failure to take appropriate steps to prevent the technical measures taken from causing health hazards to the population or from polluting the external environment and failure to regularly check the persisting absence of hazards;
 - failure to communicate to the relevant authorities, as appropriate, for statistical and information purposes, the data regarding accidents at work that involve an absence from work of at least one day, excluding the day when the event occurred, and, for insurance purposes, the information on accidents at work involving an absence from work of more than three days;
 - failure to consult the Workers' Health and Safety Representative in the cases referred to in article 50 of Legislative Decree 81/08;
 - failure to take the measures needed to prevent fires and to evacuate workplaces, as well as in the event of serious and immediate dangers according to article 43 of Legislative Decree 81/08;
 - failure to apply the penalties envisaged in procurement contracts in case of breaches, by contractors, of the rules contained in this Organisation and Management Model and of the regulations on health and safety at work;
 - failure to convene the regular meeting referred to in article 35 of Legislative Decree 81/08;
 - failure to update prevention measures following organisational and production changes that affect health and safety at work or the evolution of prevention and protection techniques;
 - failure to provide INAIL with the names of the Workers' Health and Safety Representatives;
 - failure to ensure that workers who are placed under health surveillance are not assigned a specific job duty without the prescribed assessment of their fitness;
- g) the Board of Directors and the Surveillance Body of the Foundation verify, by requesting any documents and/or gathering information from the various subjects included in the health and safety organisational chart, that the Employer regularly monitors the performance of the delegated activities and that he intervenes directly if (s)he finds any omissions by the delegate;
- h) The Surveillance Body reports, on an at least annual basis, to the Board of Directors the outcomes of its own supervising and monitoring activity;
- i) the Board of Directors, if it finds serious and/or repeated omissions to check and/or violations committed by the Employer, has him/her replaced and/or has the penalties envisaged by this Organisation and Management Model imposed on him/her.

In compliance with the provisions of the Circular Letter of the Italian Ministry of Labour and Social Policies - General Directorate for the Protection of Labour Conditions - Division VI - of 11 July 2011, concerning the definition of "suitable methods to punish external collaborators, contractors, suppliers and other subjects with contract relationships with the company itself" also by including "specific application clauses with reference to the requirements and behaviours demanded and the sanctions applicable to failure to comply, up to the termination of the contract itself", the Foundation has established specific clauses, ensuring that they are included in its agreements with third parties, which are aimed at guaranteeing their commitment to comply with, according to the type of contract relationship, the principles and procedures/rules of conduct specified in the said Organisation and Management Model applicable to them, whose violation may also entail, in the most severe cases, the contract termination.

SECTION G – CRIMES OF HANDLING STOLEN GOODS, MONEY-LAUNDERING AND USING MONEY, GOODS OR ASSETS OF UNLAWFUL ORIGIN, AS WELL AS SELF-LAUNDERING AND CRIMES OF TERRORISM AND SUBVERSION OF THE DEMOCRATIC ORDER

G 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the crimes of handling stolen goods, money-laundering, and use of money, goods or other assets of unlawful origin which are briefly described below and referred to in Articles 25-octies of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Handling stolen goods, as provided for in article 648 p. c., consists in the conduct of anyone who, in order to reap a profit for himself/herself or others, buys, receives or conceals money or goods resulting from any offence, or, however, play a role in their purchase, receipt or concealment. The provisions of this article also apply when the perpetrator from whom the money or goods are obtained is neither chargeable nor criminally liable, or when no condition for the admissibility of that offence exists;

Money-laundering, as provided for in article 648-bis p. c., consists in the conduct of anyone who, except for cases of participation in the crime, replaces or transfers money, goods or assets resulting from an offence committed with criminal intent, or performs other operations with them so as to prevent their criminal origin from being discovered;

Use of money, goods, or assets of unlawful origin, as provided for in article 648-ter p. c., consists in the conduct of anyone who, except in the cases of participation in the crime and of handling stolen goods and money-laundering, invests money, goods or other assets resulting from a crime in economic or financial activities;

Self-laundering, as provided for in article 648-ter 1, consists in the conduct of anyone who, having committed or participated in an offence with criminal intent, employs, replaces, transfers money, goods or assets resulting from that offence in economic, financial, entrepreneurial or speculative activities, so as to materially hamper the identification of their criminal origin. The conduct whereby the money, goods or other assets are meant to be merely used or enjoyed personally is not criminally liable.

G 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk and Control Self-Assessment, as available in its records, the Foundation identified sensitive activities within which some of the crimes of handling stolen goods, money-laundering, and use of money, goods or assets of unlawful origin set forth in article 25-octies of the Decree may be committed.

The sensitive activities identified by that Risk and Control Self-Assessment and shown in a table containing the description of each activity, of the corporate functions involved, of the relevant offences and showing *ad-hoc* examples of potential illegal conduct are listed below. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for such offences as USE OF MONEY, GOODS OR ASSETS OF UNLAWFUL ORIGIN, SELF-LAUNDERING
15	Marketing - Management of gifts	General Secretariat	1) Article 648-ter p. c. Use of money, goods or assets of unlawful origin 2) Article 648-ter 1 p. c. Self-laundering	1) Management of gifts, hospitality, sponsorships and charitable donations by using money from previous illegal activities 2) Any support to criminal activities may be lent, for instance, by making payments (e.g. for sponsorships, charitable donations) with money deriving from an offence with criminal intent which an executive or subordinate employee of the Foundation committed or participated in its commission (e.g. illegal financial operations, corruption, money-laundering, etc.) in order to materially hamper the identification of its criminal origin
19	Search and selection of suppliers	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of assets of unlawful origin 2) Use of money of unlawful origin for the purchase of goods or services
20	Management of relationships and of intragroup operations (e.g. execution and performance of intragroup contracts; intragroup purchases and sales)	General Secretariat	1) Article 648-bis p. c. Money-laundering 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin 3) Article 648-ter 1 p. c. Self-laundering	1) Collecting sums of money resulting from a crime and pay one of the Foundations of the Group, in exchange for a service, with that money in order to conceal its origin. Using Intercompany invoices to launder money of unlawful origin. 2) Using funds of an illegal origin to make payments to a Foundation of the Group, then investing those funds within the Foundation's economic activities. 3) Managing transfer pricing/recharges improperly, also jointly with other Foundations of the Group, investing money resulting from that offence in economic, financial, entrepreneurial and/or speculative activities, including intragroup, so as to materially hamper their criminal origin.
21	Management of the awarding of supply contracts for goods and/or services (tender / direct negotiation)	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of goods of unlawful origin 2) Use of money of unlawful origin for the purchase of goods
22	Preparation, conclusion and transmission of a contract/purchase order	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of goods of unlawful origin 2) Use of money of unlawful origin for the purchase of goods
23	Designation and monitoring of suppliers	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Failure to detect irregularities committed by suppliers of goods of unlawful origin 2) Failure to detect irregularities committed by suppliers who accept payments in cash or methods of payment facilitating the concealment of money deriving from an offence committed with criminal intent
24	Receiving goods and services and authorising payments	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of goods of unlawful origin 2) Use of money of unlawful origin for the purchase of goods
26	Designation and monitoring of IT outsourcers	General Secretariat	1) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Failure to detect irregularities when dealing with outsourcers who accept payments in cash or methods of payment facilitating the concealment of money from offences committed with criminal intent

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for such offences as USE OF MONEY, GOODS OR ASSETS OF UNLAWFUL ORIGIN, SELF-LAUNDERING
27	Designation and monitoring of administrative outsourcers	General Secretariat	1) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Failure to detect irregularities when dealing with outsourcers who accept payments in cash or methods of payment facilitating the concealment of money from offences committed with criminal intent
28	Preparation and transmission of purchase requests	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of goods of unlawful origin 2) Use of money of unlawful origin for the purchase of goods
29	Conclusion of passive lease contracts	General Secretariat	1) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Using money of unlawful origin to pay leasing contracts
31	Management of routine and emergency, scheduled and unscheduled maintenance operations	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of goods of unlawful origin 2) Use of money of unlawful origin for the purchase of goods
32	Management of compliance and upgrading activities of real estate properties	General Secretariat	1) Article 648 p. c. Handling stolen goods 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin	1) Purchase of goods of unlawful origin 2) Use of money of unlawful origin for the purchase of goods
40	Management of current accounts (opening, closing, changing specimens of signature, etc.)	General Secretariat	1) Article 648-bis p. c. Money-laundering 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin 3) Article 648 p. c. Handling stolen goods	1) Management of current accounts in order to transfer money or other assets resulting from an offence committed with criminal intent by methods that are materially suitable for hampering the identification of their illegal origin 2/3) Setting up current accounts to manage money of unlawful origin and the purchase of goods resulting from crimes
41	Management of payments and disbursements (e.g. entering invoices, creating payment orders)	General Secretariat	1) Article 648-bis p. c. Money-laundering 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin 3) Article 648 p. c. Handling stolen goods 4) Article 648-ter 1 p. c. Self-laundering	1) Replacing or transferring money or other assets resulting from an offence committed with criminal intent, by collecting and subsequently reinvesting money/assets by methods materially suitable for hampering the identification of their illegal origin 2) Using money of unlawful origin for funding projects 3) Using money for purchasing goods resulting from crimes 4) Making payments by investing money resulting from an offence with criminal intent that an executive or subordinate employee of the Foundation committed or participated in committing in order to materially hamper the identification of its criminal origin

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct for such offences as USE OF MONEY, GOODS OR ASSETS OF UNLAWFUL ORIGIN, SELF-LAUNDERING
42	Management of petty cash	General Secretariat	1) Article 648-bis p. c. Money-laundering 2) Article 648-ter p. c. Use of money, goods or assets of unlawful origin 3) Article 648 p. c. Handling stolen goods 4) Article 648-ter 1 p. c. Self-laundering	1) Replacing or transferring money or other assets resulting from an offence committed with criminal intent, by collecting and subsequently reinvesting money/assets through methods materially suitable for hampering the identification of their illegal origin 2) Use of money of unlawful origin for the purchase of goods 3) Use of money for purchasing goods resulting from crimes 4) Making payments by investing money resulting from an offence with criminal intent that an executive or subordinate employee of the Foundation committed or participated in committing in order to materially hamper the identification of its criminal origin
45	Processing of tax, social security and nursing statements	General Secretariat	1) Article 648-ter 1 p. c. Self-laundering	1) Incorrect processing of tax returns in order to enjoy lower taxation and, as a consequence, generate more proceeds to be recycled in activities of the Foundation
46	Preparation and approval of payment/statement forms	General Secretariat	1) Article 648-ter 1 p. c. Self-laundering	1) Incorrect preparation and approval of payment/statement forms in order to enjoy lower taxation and, as a consequence, generate more proceeds to be recycled in activities of the Foundation
47	Determination of direct and indirect taxes	General Secretariat	1) Article 648-ter 1 p. c. Self-laundering	1) Incorrect preparation and approval of payment/statement forms in order to enjoy lower taxation and, as a consequence, generate more proceeds to be recycled in activities of the Foundation

Internal

G 3. GENERAL PRINCIPLES OF CONDUCT

In general and in order to prevent the crimes of handling stolen goods, money-laundering, and use of money, goods or assets of unlawful origin that are relevant for the Foundation, as envisaged by the Decree, the Addressees of the Model, without prejudice to the Group Code of Conduct and to its implementing provisions, are

- required to:
 - abstain from engaging in or adopting preliminary behaviours and/or actions that may constitute the offences specified in articles 25-octies of the Decree
 - obtain adequate knowledge about the beneficiary entities, being aware that this is a precondition for preventing the use of the financial system for money-laundering and for establishing relationships with individuals linked to terrorist/subversive organisations;
 - ensure that the relevant laws and regulations in force in every geographical and operational context, as well as the operating procedures adopted by the Foundation to comply with external laws, are abided by;
 - point out and immediately report the operations conducted by or for an individual on behalf or for the benefit of third parties without family ties or trade relations justifying them, or, additionally, operations conducted by third parties for the benefit of customers without any valid reasons;
 - avail themselves, in order to implement the decisions on investing financial resources, only of financial and banking intermediaries who are bound by transparency and fairness standards complying with EU rules;
 - block or, however, abstain from implementing transactions that involve individuals / Countries / goods under financial restrictions (freezing of goods and resources, prohibitions of financial transactions, restrictions on export or investment credits) and/or trade restrictions (general or specific trade sanctions, importing and exporting bans, e.g. arms embargoes);
 - digitally certify only claims for payment coming from subjects holding delegated powers in line with the corporate organisation;
 - allow the use of computer systems for treasury management in line with the corporate organisation;
- they are also prohibited from:
 - purchasing, receiving or concealing money or things resulting from any crime in order to reap a profit for themselves or others, or, however, playing a role in or favouring their purchase, receipt or concealment;
 - replacing or transferring money, goods, or other assets resulting from an offence committed with criminal intent or from performing other operations with them so as to prevent its criminal origin from being identified;
 - investing money, goods, or other assets gained through offences committed with criminal intent in economic and financial activities

G 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

The following table lists the sensitive activities specifying, for each of them, the corporate functions involved, the relevant internal regulations (e.g. GIRS), as well as other internal procedures (e.g. operating instructions, internal manuals).

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
40	Management of current accounts (opening, closing, changing specimens of signature, etc.)	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
41	Management of payments and disbursements (e.g. entering invoices, creating payment orders)	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
42	Management of petty cash	General Secretariat	- Group Anti-Money-Laundering & Counter Terrorism Financing Policy - Group Treasury Policy - Group Treasury Guideline	
47	Determination of direct and indirect taxes	General Secretariat	- Group Tax Guideline on Foreign Entities - Group Tax Control Framework Guideline	

Internal

G 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to the contents of the table in the previous paragraph, the Foundation puts in place additional control safeguards, also for preventing the risk that the offences envisaged by the Decree and dealt with in this Section G might be committed.

They are shown below, with direct reference to the corporate functions involved.

With regard to the sensitive activities in which the **Corporate Tax Affairs** function is involved, the following control safeguards have been identified:

- the employees of the Corporate Tax Affairs structure perform their activities based on written proxies. When they act for other Group companies, they need specific written proxies authenticated by a notary public.
- in the event of extraordinary activities (e.g. start of the assessment procedure with enrolment), opinions need to be shared with the head of the Group Tax Affairs structure and with the Chief Financial Officer
- segregation of tasks between those who, within the “Tax” structure of GBS, calculate direct and indirect taxes and those who check whether they are correct within the Corporate Tax Affairs structure.

With regard to the sensitive activities in which the **Group Treasury** function is involved, the following control safeguards have been identified:

- management of payments through the SAP software
- monitoring the balance of the individual current accounts managed by each entity (as part of cash pooling activities) by using the Quantum environment;
- segregation of tasks between those who prepare claims for payment, those who authorise the payments and those who transmit the claims to the bank;
- segregation of tasks between those who request opening / changing a current account and those who authorise it;
- automatic lock of claims for payment, on the corporate IT system used to process them, if the payment recipient is different from the contract counterparty (the system, indeed, allows preparing claims for payment only by coupling them with existing invoices, which are in turn connected with a counterparty appearing in the master data or with an employee who is actually included in the master data for the payment of salaries) or manual verification, if not performed automatically by the system;
- verification of the correct authorisation of claims;
- profiling users, within the corporate IT system used for managing claims for payment, which ensures that the data contained in the claims for payment to be transmitted to banks are correct (disabling any changes to claims for payment made after their certification);
- profiling users, within the corporate IT system used for managing claims for payment, ensuring an adequate segregation of activities (those who prepare claims for payment cannot authorise them and those who authorise claims for payment cannot prepare them);
- regular monitoring of users in order to ensure that their profiles are consistent with existing delegations and powers of attorney;
- system block for entering orders of payment for the operators of the structure;
- expense reconciliation mechanisms;
- existence of a current account reserved for petty cash transactions;
- existence of a limited list of subjects authorised to withdraw money from a bank branch.

Finally, it should be noted here that, as stated in the General Part (Chapter 1, paragraph 4 Structure of the Model), with regard to crimes of terrorism and subversion of the democratic order (article 25-quater of the Decree), in view of the main activity conducted by the Foundation, of the social-economic environment in which it operates and of the legal and economic relationships it usually establishes with third parties, there are no risk profiles which make the possibility of perpetrating those crimes in the interest or for the benefit of the Foundation reasonably well-founded. Against this background, in addition to the principles enshrined in the Code of Conduct which always bind the addressees to respect basic ethical values (e.g. solidarity, respect for the human person, morality, fairness and legality), the application of the “Group Policy on Money-Laundering and on Combating Terrorist Financing” and the “Policy on International Financial Sanctions” is a further control safeguard contributing to mitigating the risk, albeit remote, of perpetration of the offences with purposes of terrorism and subversion of the democratic order specified in the Decree (e.g. both domestic and international terrorist groups, or associations aiming to subvert the democratic order, according to article 270-bis p. c.).

SECTION H - COPYRIGHT VIOLATIONS

H 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the offences for copyright violation which are briefly described below and referred to in Articles 25-novies of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Protection of copyright and connected rights, as provided for in articles 171 and 171-bis of Law no. 633 of 22 April 1941.

Article 171, paragraph 1, letter a-bis) refers to the conduct of anyone who, without being entitled, for whichever purpose and in whichever form, makes available a protected intellectual work or part thereof to the public, by uploading it, by whatever type of connection, to a data communication network system.

Article 171-bis refers to the conduct of anyone who unlawfully duplicates, in order to gain profit, computer programs or imports, distributes, sells, holds for commercial or entrepreneurial purposes or leases programs on digital devices without the SIAE marking (Italian Society of Authors and Publishers) for the same intent; uses any means allowing or facilitating the removal or circumvention of software protections; in order to gain profit, by using IT devices without the SIAE marking, transfers to another device, distributes, communicates, displays or shows the contents of a database in public, extracts or reuses, distributes, sells or leases out a database.

H 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk Self-Assessment, as available in its records, the Foundation identified sensitive activities within which some of the copyright violation offences specified in article 25-novies of the Decree may be committed.

The sensitive activities identified within that Risk Self-Assessment and shown in a table containing a description of each activity, of the corporate functions involved, of the relevant offences and showing *ad-hoc* examples of potential illegal conducts are listed below. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Examples of potential unlawful conduct related to OFFENCES FOR COPYRIGHT VIOLATIONS ¹³
6	Management of operational marketing by preparing brochures and information material on products on offer	General Secretariat	1) Production and publication of brochures and/or institutional information material (for the products on offer) by violating intellectual property rights Launching advertising campaigns, using videos or images protected by copyright without the necessary authorisations, in the interest or for the benefit of the Foundation (e.g. cost savings deriving from the failure to pay the fees set by law)
7	Management of public relations (also with public figures) and communication and marketing activities (advertising, promotional events, media corners, sponsorships, etc.)	General Secretariat	1) Unlawfully duplicating intellectual work to reduce the costs of purchasing original copies
12	Management of corporate software systems	General Secretariat	1) Installation of licences for corporate software or applications on a greater number of machines than allowed, or by circulating or reproducing programs on media without the SIAE marking
13	Management of access, accounts and profiles (for instance: for management and administrative/accounting software; for Internet access and e-mail use; for the management of credentials of system administrators, etc.)	General Secretariat	1) Installation of licences for corporate software or applications on a greater number of machines than allowed, or by circulating or reproducing programs on media without the SIAE marking

¹³ The examples of unlawful conduct concerning of copyright violation offences listed in the table refer to the offences defined in articles: 1) Article 171, paragraphs 1, letter a-bis, and 3 and article 171-bis of Law 633/41.

H 3. GENERAL PRINCIPLES OF CONDUCT

In general, and in order to prevent the perpetration of copyright violation offences and unlawful processing of relevant data for the Foundation as envisaged by the Decree, the Addressees of the Model – without prejudice to the Group Code of Conduct and to its implementing provisions are

- required to:
 - abstain from engaging in or participating in behaviours that may constitute the offences set forth in the Law on Copyright;
 - abstain from engaging in behaviours that, although they do not constitute, *per se*, any of the offences specified in the previous paragraph, may become suitable for committing those same offences;
 - regulate all purchases of hardware and software through specific agreements signed by the main manufacturers or concluded with suppliers authorised by them, containing specific clauses on copyright protection;
- they are also prohibited from:
 - installing software not authorised by the Foundation on corporate computers;
 - installing work protected by copyright on a greater number of devices than the number of purchased licences;
 - duplicating and/or installing software beyond the provisions of the agreements signed with the main manufacturers or with suppliers authorised by them;
 - duplicating and/or installing work protected by copyright without the SIAE marking or with a counterfeit marking (e. g. books, magazines, CDs, etc.)
 - reproducing (permanently or temporarily, in whole or in part), translating, adapting, transforming, distributing software owned by third parties that has been licensed without authorisation;
 - reproducing images, logos, sounds and, more generally, work protected by copyright in the documents or on the website of the Foundation without having paid their respective rights or agreed on their use with their legitimate owners;
 - disseminating, without authorisation, by uploading them to an IT network system, through connections of any kind, intellectual work protected by copyright or parts thereof;
 - reproducing, transferring to other media, distributing, communicating, exhibiting or displaying in public the contents of a database without obtaining the necessary authorisation from the legitimate owner of the copyright and/or of the right to the economic exploitation of the database.

H 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

Each outsourcer, for the sensitive activities specified in paragraph H 2, defined its own relevant internal regulations (e.g. GIRS) as well as other internal procedures (e.g. operating instructions, internal manuals etc.) or further control safeguards.

H 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to the information contained in the table in the previous paragraph, no additional control safeguards have been found during the Risk Self-Assessment activities.

SECTION I – INSTIGATION NOT TO TESTIFY OR TO GIVE FALSE TESTIMONY BEFORE COURT AUTHORITIES

I 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the crimes of instigation not to testify or to give false testimony before Court Authorities which are briefly described below and referred to in Articles 25-decies of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Instigation not to testify or to give false testimony before Court Authorities, as provided for in article 377-bis p. c., consists in the conduct of anyone who – except where the deed constitutes a more serious offence – by using violence or threat, or by offering or promising money or other benefits, induces an individual who has been called to testify before a Court Authority not to testify or to give false testimony in a criminal proceeding, when that individual has the right to remain silent.

I 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

As in the case of organised crime, the offence referred to in article 377-bis p. c. is unrelated to specific entrepreneurial activities conducted by the Foundation itself and cannot be included into a specific system of controls, provided that the crimes of instigation not to testify or to give false testimony before Court Authorities can be committed at every corporate level and in a virtually endless number of ways.

Having said that, we believe that the General principles of conduct (see paragraph I 3.) are adequate to prevent the perpetration of those offences.

The sensitive activities identified within the Risk Self-Assessment and shown in a table containing a description of each activity, of the corporate functions involved, of the relevant offences and showing *ad-hoc* examples of potential illegal conducts are listed below. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct of INSTIGATION NOT TO TESTIFY
39	Management of in and out-of-court litigations (civil, criminal, administrative, labour law cases)	General Secretariat	1) Article 377-bis p. c. Instigation not to testify or to give false testimony before court authorities	1) Using violence or threats or offering money to suspects/defendants in criminal proceedings (or to their next of kin) to convince them to give false testimony to Court Authorities in the interest or for the benefit of the Foundation (e.g. to avoid involving the Foundation or its representatives in the criminal proceedings or to favour its position within them)

I 3. GENERAL PRINCIPLES OF CONDUCT

In general and in order to prevent the offences of instigation not to testify or to give false testimony before Court Authorities from being committed, which are relevant for the Foundation, as envisaged by the Decree, the Addressees of the Model, without prejudice to the Group Code of Conduct and to its implementing provisions, are

- required to:
 - report the waivers, violations or suspected violations of the regulations governing the activities at risk described in this Special Part;
 - provide true testimony, without prejudice to the guarantees required by law, if the Court Authority hears the subjects identified as Addressees of the Model.
- The members of corporate bodies, the employees or collaborators of the Foundation, or other subjects not strictly related thereto are forbidden from instigating the Addressees of the Model through instructions, pressure, threats and/or promises of benefits not to testify or to give false testimony before Court Authorities to reap an interest or advantage for the Foundation.

I 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

Each outsourcer, for the sensitive activities specified in paragraph I 2, defined its own relevant internal regulations (e.g. GIRS), as well as other internal procedures (e.g. operating instructions, internal manuals etc.) or further control safeguards.

I 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to what is shown in the table in the previous paragraph, it should be emphasised that Assicurazioni Generali (the company seconding the Foundation's resources) puts in place additional control safeguards with the same goal of preventing the risk that the offences envisaged by the Decree and dealt with in this Section I might be committed.

With regard to the sensitive activities in which the **Group Legal Affairs** function is involved, the following control safeguards have been identified:

- specific delegations have been envisaged both for the signature of the power of attorney to appear in court (based on the value of the dispute) and for the settlements of any pending disputes;
- implementation of a Legal Panel, i.e. a list of lawyers selected by the Foundation and grouped by competencies;
- constant monitoring of the progress of individual disputes and of the actual implementation of the procedural strategy shared with the appointed lawyers;
- filing of the documentation on single disputes;
- regular assessment of the lawyers' performance based on specific criteria in order to assess their permanence in or exclusion from the panel.

SECTION J – ENVIRONMENTAL CRIMES

J 1. RELEVANT OFFENCES FOR THE FOUNDATION

For the purposes of this section, in view of the activities that the Foundation carries out on its real estate portfolio, also with the aid of some outsourcers (e.g. Generali Business Solutions S.C.p.A., Generali Real Estate S.g.r.), a dual liability profile may be envisaged:

1. with regard to the real estate properties and assets used directly by the Foundation (e.g. office buildings, tools and equipment), the risks of committing the offences described in this section can be mainly identified in management activities of hazardous and non-hazardous waste (e.g. risks related to the disposal of printer toner, electronic devices) and in activities that may constitute violations of the regulations for the protection of ozone in the stratosphere (e.g. risks related to outsourcing the maintenance of air conditioning systems);
2. with reference to premises owned or leased, the risks of perpetration of the crimes described in this section can be mainly found in the construction, maintenance, demolition, restoration activities of the said premises.

Having said that, based on the analyses conducted, the environmental crimes which are briefly described below and referred to in Articles 25-undecies of the Decree, are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Negligent crimes against the environment, as provided for in article 452-quinques p. c. occur when significant and measurable impairment or deterioration of water or air, or of vast or significant portions of soil or subsoil, of an ecosystem, of biodiversity – including agricultural – of flora or fauna are caused as a result of negligence.

Offences related to waste management, as provided for in article 256, paragraphs 1, 3, 5 and 6 of Legislative Decree 152/2006, which are committed in the following cases:

- collection, transport, recovery, disposal, commerce and brokerage of waste, both dangerous and non-dangerous, without the required authorisation, enrolment or notice (paragraph 1);
- setting up or managing an authorised landfill, possibly destined for the disposal of hazardous waste (paragraph 3)
- mixing waste without authorisation (paragraph 5);
- temporary storage at the site of production of hazardous medical waste in violation of article 227, paragraph 1, letter b) of Legislative Decree 152/2006 (paragraph 6, first sentence).

Pollution of soil, subsoil, surface or ground waters, as provided for in article 257, paragraphs 1 and 2 of Legislative Decree 152/2006, consists in the conduct of anyone who causes pollution to the soil, subsoil, surface or ground waters, by exceeding the risk threshold concentrations and does not notify the relevant authorities within the appropriate time limit or does not reclaim the site according to the plan approved by the relevant authorities.

Violation of the obligations of notification and keeping of mandatory registers and forms, as provided for in article 258, paragraph 4 of Legislative Decree 152/2006, consists in the inclusion, in a waste analysis certificate, of false information on the nature, composition and chemical-physical characteristics of the waste itself, or in the use of a false certificate during transport.

Illegal traffic in waste, as provided for in article 259, paragraph 1 of Legislative Decree 152/2006, consists in any shipment of waste which is deemed to be illegal traffic according to article 26 of Council Regulation (EEC) no. 259 of 1 February 1993, or in any shipment of waste listed in Annex II of the said regulation in breach of its article 1, paragraph 3, letters a), b), e) and d).

Organised activities for illegal traffic in waste, including highly radioactive waste, as provided for in article 260, paragraphs 1, and 2 of Legislative Decree 152/2006, are committed in the following cases:

- transfer, reception, transport, export, import or, however, unlawful management of large amounts of waste, with multiple operations and by setting up organised continuous means and activities in order to reap a wrongful profit (paragraph 1);
- in the event that the waste specified in paragraph 1 is highly radioactive.

Forgery of a waste analysis certificate used within the waste traceability control system (SISTRI), use of a fraudulently altered certificate or hardcopy of the SISTRI form, as provided for in article 260-bis, paragraphs 6, 7 and 8 of Legislative Decree 152/2006, is an offence that applies to the following cases:

- while preparing a waste analysis certificate, which is used within the waste traceability control system, false information is provided on the nature, composition, and chemical-physical characteristics of the waste, and a false certificate is included among the data to be provided for waste traceability purposes (paragraph 6);
- the carrier transporting the waste fails to exhibit a hardcopy of the SISTRI form - Handling Area and, where required

by current regulations, a copy of the analytical certificate identifying the characteristics of hazardous waste (paragraph 7);

- during transport, a waste analysis certificate is used, containing false information on the nature, composition and chemical-physical characteristics of the transported waste (paragraph 7);
- the carrier transporting the waste (either hazardous or non-hazardous) exhibits a fraudulently altered hardcopy of the SISTRI - Handling Area form (paragraph 8).

Offences concerning ozone protection, as provided for in article 3, paragraph 6 of Law no. 549 of 28 December 1993, consist in the following activities: producing, consuming, importing, exporting, holding, and marketing substances that deplete the ozone layer in the stratosphere.

Some of the categories of offences envisaged by the Decree have not been considered applicable to this model, since the Foundation does not engage in the activities specified by them (e.g. negligent or intentional pollution of marine waters) or are considered only potentially applicable and, however, adequately monitored by the safeguards implemented by the Foundation, as specified in this Model.

J 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk Self-Assessment, which is available in its records, the Foundation has identified sensitive activities, as listed below, within which some of the environmental crimes set forth in article 25-undecies of the Decree may be committed.

The sensitive activities identified within that Risk Self-Assessment and included in a table containing a description of each activity, of the corporate functions involved, of the supposedly relevant predicate offences, with examples of potential illegal conduct applying to this category of offences are listed below.

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct
AMB 1	Purchase management: selection and evaluation of suppliers	Group Chief Operating Officer [Assicurazioni Generali] /Logistics, General Services and Facility Management (GBS)	<ul style="list-style-type: none"> - Article 452 quinquies p. c. Negligent crimes against the environment - Article 257, paragraphs 1 and 2 of Legislative Decree 152/2006 Pollution of soil, subsoil, surface or underground waters - Article 256, paragraphs 1, 3, 5 and 6 of Legislative Decree 152/2006 Offences related to waste management - Article 260-bis, paragraphs 6, 7 and 8 of Legislative Decree 152/2006 Forgery of a waste analysis certificate used within the waste traceability control system (SISTRI), use of a fraudulently altered certificate or hardcopy of the SISTRI form - Article 3, paragraph 6 of Law no. 549 of 28 December 1993 Offences concerning ozone protection 	<ul style="list-style-type: none"> - In order to achieve cost savings, making use of suppliers who, lacking adequate technical and professional skills and failing to comply with ordinary good operating practices, cause damage to the environment while carrying out plant maintenance operations. - In order to achieve cost savings, within the management of own hazardous and non-hazardous waste (e.g. printer toner, electronic equipment waste), making use of suppliers who perform activities of collection, transport, recovery, disposal, commerce and brokerage of waste without the required authorisation, enrolment or notification. - In order to achieve cost savings, making use, for waste characterisation purposes, of analysis laboratories without any evidence of their reliability (e.g. accreditations issued by third parties acknowledged both domestically and internationally). - In order to achieve cost savings, making use of suppliers conducting the following activities: producing, consuming, importing, exporting, holding, and marketing substances that deplete the ozone layer in the atmosphere.
AMB 2	Production management, monitoring waste handling and storage.	Group Chief Operating Officer [Assicurazioni Generali] /Logistics, General Services and Facility Management (GBS)	<ul style="list-style-type: none"> - Article 256, paragraphs 1, 3, 5 and 6 of Legislative Decree 152/2006 Offences related to waste management - Article 258, paragraph 4 of Legislative Decree 152/2006 Violation of the obligations to keep the mandatory registers and forms - Article 259, paragraph 1 of Legislative Decree 152/2006 Organised activities of illegal traffic in waste - Article 260, paragraphs 1, and 2 of Legislative Decree 152/2006 Organised activities for illegal traffic in waste, including highly radioactive waste - Article 260-bis, paragraphs 6, 7 and 8 of Legislative Decree 152/2006 Forgery of a waste analysis certificate used within the waste traceability control system (SISTRI), use of a fraudulently altered certificate or hardcopy of the SISTRI form 	<ul style="list-style-type: none"> - Performing, also in collaboration with others, such activities as collection, transport, recovery, disposal, commerce and brokerage of own hazardous and non-hazardous waste (e.g. printer toner, electronic equipment waste) without the required authorisation, enrolment or notification. - Organising shipments of waste constituting illegal traffic under article 26 of (EEC) Regulation no. 259 of 1 February 1993. - Unlawfully manage large amounts of waste, in order to reap a wrongful profit, with multiple operations and by using appropriate vehicles and continuous organised activities. - Providing false information on the nature, composition, and chemical-physical characteristics of the waste while preparing a waste analysis certificate, which is used within the waste traceability control system.

Internal

ID	Description of the sensitive activity	Corporate functions involved	Relevant offences	Examples of potential unlawful conduct
AMB 3	Management of the maintenance of equipment and buildings.	Group Chief Operating Officer [Assicurazioni Generali] /Logistics, General Services and Facility Management (GBS)	<ul style="list-style-type: none"> - Article 452 quinquies p. c. Negligent crimes against the environment - Article 257, paragraphs 1 and 2 of Legislative Decree 152/2006 Pollution of soil, subsoil, surface or underground waters - Article 279, paragraph 5 of Legislative Decree 152/2006 Exceeding the emission threshold values for the operation of a facility - Article 3, paragraph 6 of Law no. 549 of 28 December 1993 Offences concerning ozone protection 	<ul style="list-style-type: none"> - In order to achieve cost savings, failing to monitor the real estate portfolio, fail to adequately schedule maintenance operations, setting, as a result, the conditions for polluting the environment (e.g. integrity monitoring referring to materials containing asbestos). - Causing the pollution of soil, subsoil, surface or underground waters for failing to implement the necessary maintenance operations (e.g. integrity monitoring and maintenance of any landfilled vessels containing hazardous liquids). - Violating the prescriptions of the authorisation to emissions in the atmosphere, by also exceeding the limit values for air quality set by current regulations. - Conducting such activities as producing, consuming, importing, exporting, holding, and marketing substances that deplete the ozone layer in the atmosphere.

Internal

J 3. GENERAL PRINCIPLES OF CONDUCT

All the Model's Addressees adopt rules of conduct in line with the general conduct principles described below in order to prevent the occurrence of environmental crimes which are relevant for the Foundation and envisaged by the Decree.

The principles contained in the Group Code of Conduct, which are here referenced in their entirety, are preconditions and an integral part of the general principles of conduct referred to in this paragraph, as well as of the specific principles of conduct referred to in the subsequent paragraph.

The waivers, violations or suspected violations of the regulations governing activities at risk of crimes described in this Special Part are liable to be reported by all employees and corporate bodies.

In particular, the following general principles of conduct apply:

- the Foundation **adopts** a formalised system of procedures for environmental management, in which the general goals are also established, which it plans to achieve. Those procedures:
 - contain the commitment to guarantee compliance with the applicable laws on the environment;
 - are adequately communicated to employees and stakeholders;
 - are periodically updated.
- the Foundation **adopts**, with regard to subjects who are responsible for activities potentially affecting the environment, a formal system for attributing responsibilities through delegations and proxies, which are formally accepted, while also providing for:
 - a corporate organisation chart which includes the corporate functions whose activities have a potential impact on the environment;
 - specific minimum requirements – to be verified periodically – of single functions, consistently with organisational needs and relevant law provisions (e.g. previous experience, specific qualifications, skills and training, etc.);
 - a document describing the relevant functions of the organisation's activities.
- the Foundation, also availing itself of outsourcer(s), **identifies**, documents and manages the legal or different prescriptions involving the organisation, since they can be applied to the environmental aspects of its activities, products and services, later defining their scope of possible application, by adopting a formal system defining:
 - roles and responsibilities concerning the information on relevant regulatory aspects and applicable environmental prescriptions;
 - criteria and methods for regulatory updates and for the respective communication to the corporate areas involved;
 - criteria and methods for assessing the evolution of the best practice and of environmental regulations.
- the Foundation, also through outsourcer(s), **defines**, through the specific procedure, the methods for checking the documentation regarding Environmental Management: preparation, issuance, verification, approval, distribution, maintenance and processing of obsolete documents. In particular, it defines:
 - roles and responsibilities in the management of the documentation (e.g. Manual of Procedures, Operating Instructions), in line with the relevant corporate policy;
 - methods for recording, managing, archiving and keeping the documentation produced (e.g. methods for archiving documents and entering them in the appropriate registers, thus ensuring that they are adequately traceable and verifiable).
- the Foundation, also through the outsourcer(s), adopts a procedure that regulates the process of competency, training and organisation of coaching courses, including on the environment, establishing, in particular:
 - roles and responsibilities concerning the training on environmental aspects and on the respective procedures, which all employees of the Foundation must attend;
 - criteria for updating and/or supplementing the training, considering any transfers or changes of duties, introduction of new equipment or technologies that may have significant impact on the environment, etc.;
 - contents and methods for providing training according to the role and position held within the organisational structure, in particular with regard to the functions dealing with the environment;
 - training delivery time (es. definition of a training plan).
- the Foundation, in line with applicable regulations and also through operating control instruments, also availing itself of outsourcer(s) **defines** appropriate instruments to identify and measure possible negative effects, in order to determine adequate control safeguards that can minimise those effects, while identifying, in particular, the criteria and the subjects in charge of controls.

- The identification of possible adverse effects and the assessment of their significance / criticality are conducted by considering normal operating conditions and any abnormal situations, as well the emergency situations that may be predicted based on available elements.
- the Foundation **defines** the methods for identifying and maintaining operating instructions for responding to potential accidents and emergencies that may have an impact on the environment through a specific procedure for managing emergencies which:
 - identifies the possible scenarios of environmental emergencies;
 - outlines roles, responsibilities and measures to control emergency situations;
 - identifies suitable measures for avoiding risks for public health or for habitat pollution;
 - defines timing and methods for performing emergency tests;
 - prescribes how historical records should be kept, which contain references to the tests and simulations carried out and to the emergency situations that have occurred, in order to allow the adequacy of the response plans laid out and the traceability of the corrective actions implemented to be evaluated.
- organisational tools have been **adopted**, which define methods for selecting and checking suppliers. In particular, they define:
 - roles, responsibilities and procedures for selecting suppliers;
 - criteria for verifying the technical-professional requirements of suppliers (e.g. enrolment in the register of environmental managers for subjects overseeing waste management);
 - monitoring methods to ensure compliance with environmental regulations by suppliers, contractors and subcontractors.
- roles, responsibilities and operating methods to be **established** for conducting auditing activities on the efficiency and effectiveness of the environmental management system, as well as methods for:
 - identifying and applying corrective actions and actions to verify their actual implementation;
 - providing the results to the Top Management.

Finally, the certified environmental management system of the Foundation and its related procedures are appropriate safeguards.

J 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

The following paragraphs list the sensitive activities and indicate, for each one, the corporate functions involved, the relevant internal regulations (e.g. GIRS, Guidelines), as well as the other internal procedures (e.g. operating instructions, internal manuals).

The sensitive activities managed, in whole or in part, by the Foundation are listed below.

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
AMB 1	Purchase management: selection and evaluation of suppliers	Group Chief Operating Officer / Logistics, General Services and Facility Management (GBS)	Waste Management Policy/Guideline/Operating Procedure	<ul style="list-style-type: none"> - Definition of roles, responsibilities and procedures for selecting suppliers and subcontractors; - Preliminary verification of the technical-professional requirements of suppliers (e.g. enrolment in the register of environmental managers of subjects overseeing waste management, ACCREDIA accreditation for analysis laboratories, etc.); - Inclusion of contractual clauses imposing compliance with the applicable environmental regulations and, where necessary, of the procedures defined by the Foundation, as well as the respect for the general principles enshrined in the Model and in the Code of Conduct. - Exclusive use of suppliers enrolled in the F-GAS register.
AMB 2	Production management, monitoring waste handling and warehousing.	Group Chief Operating Officer / Logistics, General Services and Facility Management (GBS)	Waste Management Policy/Guideline/Operating Procedure	<ul style="list-style-type: none"> - Within the production, collection, transport, and disposal of waste: <ul style="list-style-type: none"> • upon defining the requirements of the products to be purchased, the management of their “end of life” is duly taken into account, steering choices towards those products that may be, in whole or in part, destined for recovery; • the reduction of the waste to be sent to landfills is favoured, promoting their recycling; • roles and responsibilities are regulated with a view to ensuring the determination of the correct codes for waste, also by identifying appropriate subjects who are able to check and analyse it; • a correct differentiation of waste and the prevention of any illegal mixing are ensured; • temporary depositories for waste are correctly managed based on the type and amount of waste produced; • any authorisations needed for conducting collection activities (e.g. storage) are evaluated and the necessary procedures for obtaining them are activated; • the monitoring of activities is planned and guaranteed, by providing supervisors with their results; • the relevant documentation is guaranteed to be available (e.g. records of analytical checks); • the roles and responsibilities are identified to ensure that the subjects identified for transporting waste meet the requirements laid down in the current regulations; • in the event of autonomous transports, compliance with the requirements prescribed by current regulations for carriers is ensured; • the correct management of fulfilments to check the transports of waste up to their arrival to their final destination is guaranteed (management of forms and loading/unloading registers, management of SISTRI forms); • the relevant documentation is guaranteed to be available (e.g. registers, forms, accompanying analytical documentation, etc.); • the roles and responsibilities are identified who ensure that the subjects identified for waste disposal meet the requirements laid down in the current regulations; • the correct management of fulfilments is ensured to check whether the disposal is conducted in compliance with the law; • the correct filling of FIR (waste identification forms) is monitored periodically, also by using databases and summaries by CER code (developed by the subject in charge of managing waste records), leading up to the correct filling of the annual MUD (unified form for environmental statement); • the relevant documentation is guaranteed to be available.

Internal

ID	Description of the sensitive activity	Corporate functions involved	Specific principles of control	
			Relevant internal regulations	Other internal procedures
AMB 3	Management of the maintenance of equipment and buildings.	Group Chief Operating Officer / Logistics, General Services and Facility Management (GBS)	Waste Management Policy/Guideline/Operating Procedure	<ul style="list-style-type: none"> - The performance of routine and scheduled maintenance operations is guaranteed - Extraordinary maintenance operations are also conducted in order to contain any environmental accidents.

Internal

J 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to the information contained in the table in the previous paragraph, no additional control safeguards have been identified during the Risk Self-Assessment activities.

SECTION K – EMPLOYMENT OF FOREIGN NATIONALS WITH IRREGULAR RESIDENCE PERMITS, ILLICIT BROKERING AND LABOUR EXPLOITATION

K 1. RELEVANT OFFENCES FOR THE FOUNDATION

Based on the analyses conducted, the offences of employment of foreign nationals with irregular residence permits, as well as those of illicit brokering and labour exploitation, which are succinctly described below, as referred to in article 25-duodecies of the Decree and in article 603-bis p. c., are considered applicable to the Foundation, however, according to article 26 of the Decree, the Foundation may still be considered liable for mere attempts to commit those crimes.

Temporary and permanent employment, as provided for in article 25-duodecies, consists in the conduct of anyone who, in his/her capacity as employer, employs foreign workers without residence permit or whose residence permits have expired without any application for renewal having been submitted within the time limits laid down by the law, or have been either withdrawn or cancelled, if the employed workers are (alternatively):

- more than three;
- minors of non-working age;
- subjected to other working conditions of particular exploitation referred to in paragraph 3 of article 603-bis p. c., i.e. they are exposed to serious dangers, with reference to their tasks assigned and working conditions.

Illicit brokering and labour exploitation, as provided in article 603-bis p. c., consists in the conduct of anyone who:

- recruits labour to employ them at third-party facilities in exploitative conditions, taking advantage of the workers' state of need;
- uses, hires or employs workers, including by means of brokering, as referred to above, exploiting them and taking advantage of their state of need

One or more of the conditions listed below are indicators of exploitation:

- repeated payment of wages manifestly below the standards set by national or local collective labour agreements concluded by the most representative national trade unions or, however, which are disproportionate compared to the amount and quality of the work;
- repeated violation of the regulations on working hours, rest periods, weekly rest day, compulsory periods of unpaid leave, and holidays;
- violations of the regulations on occupational safety and hygiene;
- submitting workers to degrading working conditions, methods of surveillance or housing conditions.

Specific aggravating circumstances are:

- a number of hired workers greater than three;
- one or more of the recruited subjects being minors of non-working age;
- exposing exploited workers to serious hazards, considering the characteristics of the tasks to be performed and the working conditions.

K 2. IDENTIFICATION OF SENSITIVE ACTIVITIES

Through a Risk Self-Assessment, as available in its records, the Foundation identified sensitive activities within which some of the offences of employment of foreign nationals with irregular residence permits, illicit brokering and labour exploitation set forth in article 25-duodecies of the Decree and article 603-bis p. c. might be committed.

The sensitive activities identified within that Risk Self-Assessment and included in a table containing a description of each activity, of the corporate functions involved, of the relevant offences and showing *ad-hoc* examples of potential illegal conducts are listed below. Any fully outsourced sensitive activities are highlighted in grey.

ID	Description of the sensitive activity	Corporate functions involved	Examples of potential unlawful conduct for OFFENCES AGAINST THE INDIVIDUAL ¹⁴	Examples of potential unlawful conduct for the crime of EMPLOYMENT OF FOREIGN NATIONALS WITH IRREGULAR RESIDENCE PERMITS ¹⁵
19	Search and selection of suppliers	General Secretariat	1) Hiring, using and employing, also through contractor/subcontractors, workers, subjecting them to exploitative conditions and taking advantage of their state of need in order to reap an economic advantage	1) Employing, including through contractors / subcontractors, third-country nationals without or with expired residence permits.
21	Management of the awarding of supply contracts for goods and/or services (tender / direct negotiation)	General Secretariat		1) Preparation and transmission of contracts/purchase orders with suppliers who employ foreign nationals with irregular residence permits in order to achieve savings for the Foundation
22	Preparation, conclusion and transmission of a contract/purchase order	General Secretariat		1) Preparation and transmission of contracts/purchase orders with suppliers who employ foreign nationals with irregular residence permits in order to achieve savings for the Foundation
23	Designation and monitoring of suppliers	General Secretariat		1) Failure to monitor or intentionally incorrect monitoring of suppliers who employ foreign nationals with irregular residence permits in order to achieve savings for the Foundation
24	Receiving goods and services and authorising payments	General Secretariat		1) Employing, including through contractors / subcontractors, third-country nationals without or with expired residence permits.
28	Preparation and transmission of purchase requests	General Secretariat		1) Preparation of purchase orders with suppliers who employ foreign nationals with irregular residence permits in order to achieve savings for the Foundation
44	Administrative management of staff (e. g. processing of payroll slips, calculation of taxes and contributions, etc.)	General Secretariat	1) Hiring, using and employing, also through contractor/subcontractors, workers, subjecting them to exploitative conditions and taking advantage of their state of need in order to reap an economic advantage	1) Employing, including through contractors / subcontractors, third-country nationals without or with expired residence permits.

¹⁴ The examples of unlawful conduct concerning offences against the individual listed in the table refer to the offences defined in articles: 1) Article 603-bis p. c. Illicit brokering and labour exploitation.

¹⁵ The examples of unlawful conduct concerning the offences of employment of foreign nationals residing illegally in Italy listed in the table refer to the offences defined in articles: 1) Article 22 of Legislative Decree 286/98 Employment of foreign nationals residing illegally.

Internal

K 3. GENERAL PRINCIPLES OF CONDUCT

In general and in order to prevent the offences of employment of foreign nationals with irregular residence permits, illicit brokering and labour exploitation that are relevant for the Foundation, as envisaged by the Decree from being committed, the Addressees of the Model, without prejudice to the Group Code of Conduct and to its implementing provisions, are

- required to:
 - abstain from engaging in or participating in conduct that may constitute, either jointly or individually, the offences specified in articles 25-duodecies of the Decree and in 603-bis p. c.;
 - abstain from engaging in or participating in behaviours that, although they do not constitute, *per se*, the offences of employment of foreign nationals with irregular residence permits, illicit brokering and labour exploitation, may contribute to committing those same offences;
- they are also prohibited from:
 - employing foreign workers without residence permits with the Foundation, including through contractors;
 - employing foreign workers, including through contractors, whose residence permits have expired and who did not apply for their renewal within the time limits laid down by the law;
 - employing with the Foundation foreign workers, also through contractors, whose residence permits have been withdrawn or cancelled;

K 4. SPECIFIC CONTROL PRINCIPLES FOR SENSITIVE ACTIVITIES

Each outsourcer, for the sensitive activities specified in paragraph K 2, defined its own relevant internal regulations (e.g. GIRS) as well as other internal procedures (e.g. operating instructions, internal manuals etc.) or further control safeguards.

K 5. FURTHER CONTROL SAFEGUARDS

In addition to the general control principles (see General Part, Chapter II, paragraph 8) and to the data shown in the table in the previous paragraph, the Foundation puts in place additional control safeguards with the same goal of preventing the risk that the offences envisaged by the Decree and dealt with in this Section K might be committed.

With regard to the sensitive activities in which the **HR BP CFO, M&A, S&BA, CM&CO, CA, Control Functions** are involved, the following control safeguards have been identified:

- archiving e formalising all the documentation (reports) generated by external companies during the assessments carried out for recruiting and promotions to executive or managers. The outcome of the assessments of candidates at various stages of the selection process is also formalised;
- Checks on hired people (e.g. collection of criminal records, check on related parties, compliance with the legislative constraints on non-EU citizens, "Fit & Proper" self-declaration).