

Management, Organisation and Control Model

Approved with the Board of Directors' resolution of 21st March 2018


 ecopneus	ECOPNEUS	Issued on: 21/03/2018 Revisione: 0.4
MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2011		

TABLE OF CONTENTS

FOREWORD

1. THE DECREE LAW 8th June 2001 N. 231
 - 1.1 The Bodies' Responsibility
 - 1.2 Offenders
 - 1.3 Crimes committed abroad
 - 1.4 Attempted offences
2. RELEVANT TYPES OF OFFENCE
3. SANCTIONS
4. THE MANAGEMENT, ORGANISATION AND CONTROL MODEL
 - 4.1 Exempting Value of the Model
 - 4.2 Exempting Eligibility of the Model
5. THE TRADE ASSOCIATIONS' GUIDELINES

GENERAL PART

6. ECOPNEUS' MANAGEMENT, ORGANISATION AND CONTROL MODEL
 - 6.1 Scope and contents
 - 6.1.2 Improvement of Governance Rules
 - 6.2 Recipients
 - 6.3 Methodological Principles and Guiding Principles
 - 6.3.1 Identification of sensitive Areas, Activities and Processes
 - 6.3.2 Risk Assessment, Gap Analysis, Action Plan
 - 6.3.3 Risk Analysis Results
 - 6.3.4 Model Preparation
 - 6.4 Model Modifications
 - 6.5 EP's Organisation
 - 6.5.1 Organisational Chart
 - 6.6 The Principles that have inspired corporate Rules and Procedures (Control System)
 - 6.7 Procedures, Company's Rules and other internal Documentation
 - 6.8 Code of Ethics
7. SUPERVISORY BODY'S ARTICLES OF ASSOCIATION
 - 7.1 Identification and operational requirements
 - 7.2 Functions and Powers
 - 7.3 Appointment, Termination, Ineligibility and Revocation
 - 7.4 Information Flows and Notifications to the Supervisory Body
 - 7.5 Reporting to Company's Bodies
 - 7.6 Supervisory Body's Meetings, Collection and Filing of Documentation
 - 7.7 Confidentiality
 - 7.8 Compensation
 - 7.9 Modifications
8. DISCIPLINARY SYSTEM
 - 8.1 Disciplinary System Function
 - 8.2 Relevant Types of Conduct
 - 8.3 General Criteria for the imposition of Sanctions and/or Protection Measures
 - 8.4 Communication of Violations and Sanctioning Procedure
 - 8.5 Sanctioning of Middle Management and Employees
 - 8.5.1 Field of Application
 - 8.5.2 Sanctions
 - 8.6 Sanctioning of Senior Management
 - 8.6.1 Field of Application
 - 8.6.2 Sanctions
 - 8.7 Administrators and General Manager (Top-ranking positions)
 - 8.7.1 Field of Application
 - 8.7.2 Protection Measures
 - 8.7.3 Sanctioning Procedure
 - 8.7.4 What happens, if a Subject holds more than one position
 - 8.8 Auditors

8.9 External Collaborators

8.9.1 Field of Application

8.9.2 Protection Measures

9. COMMUNICATION AND TRAINING

9.1 Employees' Communication and Training

9.2 Communication to Company's Bodies

9.3 Communication to external Third Parties

FOREWORD

This document is composed of three parts:

- I. The first part makes reference to the analysis of the Decree Law 8th June n. 231 (“DL. 231”);
- II. The second part (“General Part”) is about the application of the Company’s regulatory provisions. It comprises: the description of Company’s Organisation, the methodological Principles, the Principles that inspired the elaboration of the document, the Supervisory Body’s Articles of Association, and the Disciplinary System;
- III. The third part is composed of the Special Parts. Each one of them represents an area at risk of committing crimes of the described typology. Each of them describes: sensitive activities; crimes that can be conceived in theory; a reminder of preventive and operative protocols provided for; a reminder of every single detailed procedure and/or Company’s rule (already in force and previously divulged to the Structure).

The organisational chart and the descriptive crime sheets complete the Document.

The Behavioural Rules contained in this Model integrate the ones of the Code of Ethics. The Code of Ethics is an integrating part of the Model. It has been adopted by the Company in order to define the principles of its corporate ethics. All Recipients are to respect them, namely all those people who are part of the corporate organisation, and, thus: Business Partners, Administrators, Managers, Employees, Collaborators, contractual Counterparts and whoever sets up a relationship with Ecopneus, directly or indirectly, permanently or temporarily.

1. THE DECREE LAW 8th JUNE 2001 N. 231

1.1 The Bodies’ Responsibility

The Decree Law 231, “*Discipline of the administrative responsibility of the legal persons, of the companies and of the associations even without legal responsibility*”, introduced the concept of administrative liability for Institutions into the Italian judicial system for some obligatorily listed crimes, committed to their advantage or simply in their interest. Examples of Institutions may be: Companies, Legal Persons, non-recognised Collective Institutions, associations, Consortiums etc., here-below collectively known as “Bodies”.

1.2 Offenders

As per DL. 231, the Bodies are responsible for the crimes committed in their interest or to their advantage by:

- natural persons having representative, administrative or managerial roles in the same Bodies or in one of their organisational unit possessing financial and functional autonomy;
- natural persons who carry out the management and control of the same Bodies, also *de facto*;
- natural persons that are subject to the management or vigilance of one of the afore-mentioned Subjects, if the committing of the crime was made possible by the lack of vigilance.

The Body’s responsibility is added to the penal responsibility of the natural person who materially committed the crime. The Body is held responsible even in the case of an unknown offender or of an offender that cannot be held liable and in the case of extinguished crime for causes that are different from amnesty.

On the contrary, by express provision in the legislation (art. 5, comma 2, DL. 231), the Company shall not be held responsible, if the afore-mentioned people acted in their exclusive interest or in the interest of Third Parties.

1.3 Crimes committed abroad

The afore-said responsibility applies also with reference to the crimes committed abroad.

The assumptions the Body’s responsibility is based on for crimes committed abroad are listed here-below. The assumptions are provided for by the Rule, or can be inferred from the overall complex of rules and regulations of the Decree Law 231:

- I. The crime is to be committed abroad by a Subject connected to the Body as per art. 5, comma 1, of DL 231;
- II. The Body is to have its registered offices on the Italian territory;
- III. The Body can be held responsible only in the cases and at the conditions provided for by art. 7, 8, 9, 10 of the Penal Code. Moreover, in the cases in which the Law provides for that the perpetrator (a natural person) is punished upon request of the Ministry of Justice, action is taken against the Body only if the request has been formulated even towards the same Body;
- IV. Existing the cases and the conditions provided for in the above-mentioned articles of the Penal Code, the Body shall be held responsible providing the State where the crime has been committed does not take action against the same Body;
 - I. In any case, the crime must be included among the ones expressly stated by DL 231, according to the principles of legality, as per art. 2 of DL 231.

1.4 Attempted offences

In the case of attempted committing of the crimes described in Chapter I of the DL 231, the financial penalties (in terms of amounts) and the interdiction sanctions (in terms of time) are reduced by a third to half of the amounts. On the contrary, the application of sanctions is excluded in those cases in which the Body voluntarily prevents the committing of the offence or the happening of the event.

2. RELEVANT TYPES OF OFFENCE

The relevant types of offence – as per DL 231 and its following modifications – in order to configure the Body's administrative liability, are the ones expressly provided for by the Legislator, in respect of the principle of legality and confirmed by art. 2 of DL 231. For the sake of convenience, they can be comprised in the following categories:

Crimes with reference to the relationship with the Public Administration

- Embezzlement damaging the State or any other Public Body (art. 316 bis, Penal Code)
- Misappropriation of contributions, financing or other disbursement from the part of the State or of any other Public Body (art. 316 *ter.*, Penal Code);
- Malfeasance in office (art. 317, Penal Code)
- Corruption in the exercising of one's powers (art. 318, Penal Code);
- Corruption for an act contrary to the duties of office (art. 319, Penal Code);
- Corruption in legal proceedings (art. 319 *ter.*, Penal Code);
- Inducement to give or promise benefits (art. 319 *quarter*, Penal Code);
- Corruption of person in charge of public service (art. 320, Penal Code);
- Inducement to corruption (art. 322, Penal Code);
- Misappropriation, malfeasance, corruption and inducement to corruption of members of the European Community's or Foreign Countries' Bodies (art. 322 bis, Penal Code);
- Fraud against the State or any other Public or European Community's Body (art. 640, co. 2 n. 1, Penal Code);
- aggravated fraud for the obtaining of public disbursement (art. 640 *bis*, Penal Code);
- IT fraud against the State or any other Public Body (art. 640 *ter.*, Penal Code);

IT crimes and illicit data management

- Illegal access to an IT system (art. 615 *ter.*, Penal Code);
- Illegal detention and spreading of access codes to IT systems (art. 615-*quarter*, Penal Code);
- Spreading of equipment, devices or IT programmes aimed at damaging or interrupting an IT system (art. 615 *quinquies*, Penal Code);
- Illicit interception, impediment or interruption of IT communication (art. 617 *quarter*, Penal Code);
- Installation of equipment aimed at intercepting, preventing or interrupting IT communication (art. 617 *quinquies*)
- Damaging of information, data, and IT programmes (art. 635 *bis*, Penal Code);
- Damaging of information, data, and IT programmes used by the State or by any other Public Body or, in any case, of Public Utility (art. 635 *ter.*, Penal Code);
- Damaging of IT systems (art. 635 *quarter*, Penal Code);
- Damaging of IT systems of Public Utility (art. 635 *quinquies*, Penal Code);
- IT fraud of the Subject that offers electronic signature certification services (art. 640-*quinquies*, Penal Code);
- False public IT document or document having evidential efficacy (art. 491-*bis*, Penal Code);

Organized crime offences

- Crime association (art. 416 c.p.p.)
- Mafia-style crime association (art. 416 *bis* Penal Code);
- Political-mafia electoral exchange (art. 416-*ter* Penal Code);
- Kidnapping aimed at extortion or robbery (art. 630 Penal Code);
- Other crimes committed as per what provided for by art. 416-*bis* Penal Code or in order to help mafia-style criminal associations
- Association with the purpose of illegal trafficking of drugs or psychotropic substances (art. 74 D.P.R. 309/1990)
- Crime Association (art. 416, Penal Code, to the exception of paragraph six)
- Illegal fabrication, introduction into the State, sale, transfer, possession or carrying in a public or open place of weapons of war or parts of the same, of explosive, of clandestine weapons as well as more common firing weapons (art. 407, c. 2, lett. a), number 5), Code of Criminal Procedure.)

Crimes of money forging; crimes of forging of legal tender, of tax stamps and of tools or signs of recognition

- Forging of currency, expenditure and introduction of forged currency in the State through intermediaries (art. 453 Penal Code);
- Altering of currency (art. 454 Penal Code);
- Expenditure and introduction of forged currency in the State, without intermediaries (art. 455 Penal Code);
- Expenditure of forged currency received in good faith (art. 457 Penal Code);
- Forging of tax stamps, introduction in the State, purchasing, detention or spreading of forged tax stamps (art. 459 Penal Code);
- Counterfeiting of watermarked paper in use for the fabrication of legal tender or tax stamps (art. 460 Penal Code);
- fabrication or detention of watermarked paper or of tools destined to the production of currency, tax stamps or watermarked paper (art. 461 Penal Code);
- Use of counterfeited or altered tax stamps (art. 464 Penal Code);
- Counterfeiting, alteration or use of marks, distinctive signs, patents, models and designs (473 Penal Code);
- Introduction in the State and trade of counterfeited goods (474 Penal Code);

Crimes against Industry and Commerce

- Disruption of the freedom of industry or commerce (art. 513 Penal Code);
- Illicit competition with threats or violence (art. 513 *bis*, Penal Code);
- Fraud against national industry (art. 514 Penal Code);
- Fraud in the exercise of commerce (art. 515 c.p.)
- Sale of adulterated food products as genuine (art. 516 Penal Code);
- Sale of industrial goods with mendacious signs (art. 517 Penal Code);
- Fabrication and trade of goods produced usurping industrial property rights (art. 517 *ter.*, Penal Code);
- Counterfeiting of Protected Designated of Origin and of Protected Geographical Denomination of agro-alimentary goods (art. 517 –*quarter*, Penal Code);

Corporate Crime

- False corporate communication (art. 2621, Civil Code)
- False corporate communication for mild severity facts (art. 2621 *bis*, Civil Code)
- False corporate communication of Public Companies (art. 2622, Civil Code)
- False in prospect (art. 173 *bis* TUF, ex art. 2623 Civil Code)
- Prevented Control (art. 2625 Civil Code)
- Undue repayment of contributions (art. 2626 Civil Code)
- Illegal distribution of profits and reserves (art. 2627 Civil Code)
- Illicit operations on shares, on corporate shares, or on the controlling company (art. 2628, Civil Code)
- Operations to the detriment of creditors (art. 2629 Civil Code)
- Fictitious formation of capital (art. 2632 Civil Code)
- Undue distribution of company's assets from the part of liquidators (art. 2633, Civil Code)
- Corruption among private subjects (art. 2635 Civil Code)
- Instigation to corruption among private subjects (art. 2635 *bis*, Civil Code)
- Illicit influence on the Assembly (art. 2636 Civil Code)
- Insider Trading (art. 2637 Civil Code)
- Obstructing Public Supervisory Bodies' activities (art. 2638 Civil Code)
- Omitted disclosure of conflict of interest (art. 2629 *bis*, Civil Code)

Crimes with terroristic aims

- Subversive Associations (art. 270 Penal Code);
- Association with the aim of international terrorism or eversion of democratic order (art. 270 *bis*, Penal Code);
- Assistance to associates (art. 270 *ter.*, Penal Code);
- Enlisting for ends of terrorism (art. 270 *quarter*, Penal Code);
- Training to activities with aims of international terrorism (art. 270 *quinquies*, Penal Code);
- Forms of conduct with ends of terrorism (art. 270 *sexies*, Penal Code);
- Attack with purpose of terrorism or subversion (art. 280 Penal Code);
- Act of terrorism with deadly or explosive weapons (art. 280 *bis*, Penal Code);
- Kidnapping to the aim of terrorism or subversion (art. 289 *bis*, Penal Code);
- Instigation to committing one of the crimes described in Chapters one and two (art. 302 Penal Code);
- Political Conspiracy through Agreement (art. 304 Penal Code);
- Political Conspiracy through Association (art. 305 Penal Code);

- Armed Group: formation and participation (art. 306 Penal Code);
- Assistance to the participants of conspiracies or of armed groups (art. 307 Penal Code);
- Seizing, hijacking, and destruction of a plane (art. 1 Law 342/76)
- Damaging of ground installations (art. 2 Law 342/76)
- Sanctions (art. 3 Law 342/76)
- Active repentance (art. 5 DL. 625/79)
- New York's convention of 9th September 1979 (art. 2)

Crimes related to the practices of female genitalia mutilation

- Practices of female genitalia mutilation (art. 583 *bis*, Penal Code);

Crimes against individual person

- Enslavement (art. 600 Penal Code);
- Prostitution of minors (art. 600 *bis*, Penal Code);
- Pornography of minors (art. 600 *ter.*, Penal Code);
- Detention of pornographic material (art. 600 *quarter*, Penal Code);
- Virtual Pornography (art. 600 *quarter*, 1 Penal Code);
- Touristic initiatives aimed at the exploitation of pornography of minors (art. 600 *quinqüies*, Penal Code);
- Trafficking in persons (art. 601 Penal Code);
- Purchasing and alienation of slaves (art. 602 Penal Code);
- Illicit intermediations and labour exploitation (art. 603 *bis*, Penal Code);
- Grooming of minors (art. 609 *undecies*, Penal Code);

Crimes of market abuse

- Abuse of privileged information (art. 184 DL 158/98)
- Market manipulation (art. 185 e 187 *ter.* DL. 158/98)

Crimes of manslaughter and involuntary personal injury with violation of safety rules and regulations

- Manslaughter (art. 589 Penal Code);
- Involuntary personal injury committed in violation of the safety rules and of the rules in protection of the hygiene and health on the workplace (art. 590, co. 3 Penal Code);

Crimes of receiving of stolen goods, of money-laundering, and of use of money, goods and benefits of illicit provenance, as well as crimes of "self-laundering"

- Receiving of stolen goods (art. 648 Penal Code);
- Money-laundering (art. 648 *bis*, Penal Code);
- Use of money, goods, and benefits of illicit provenance (art. 648 *ter.*, Penal Code);
- Self-laundering (art. 648 *ter-1* Penal Code);

Crimes with reference to violation of copyright

- Making available to the public a work of protected intellectual property or part of the same by loading it onto an IT system by the means of any type of connection (art. 171 co. 1 lett. a *bis* e co. 3 Law 633/1941)
- Crimes with reference to software and databanks (art. 171 *bis* co. 1 e 3 Law 633/1941)
- crimes with reference to protected intellectual property destined to cinema, radio and television broadcasting, or literary, scientific and didactic protected intellectual property (art. 171 *ter.*, Law 633/1941)
- Violations of SIAE – the Italian Society of Authors and Publishers (art. 171 *septies*, Law 633/1941)
- Damaging of devices for the decoding of audio-visual signals of conditioned access (art. 171 *octies*, Law 633/1941)

Crimes against the Administration of Justice

- Instigation not to make statements or to make false statements to the Judicial Authority (377 *bis*, Penal Code);

Environmental Crimes

- Killing, destruction, capture, collection, detention of protected species of wild animals or plants (art. 727 *bis*, Penal Code);
- Destruction or deterioration of a habitat within a protected site (art. 733 *bis*, Penal Code);
- Importation, exportation, detention, use for profit, purchasing, sale, exhibition or detention for sale or for commercial aims of protected species (art. 1, 2, 3 *bis* 6 L. 150/92);

- Discharge of wastewater containing dangerous substances; discharges on the ground, in the underground and in ground water; discharge in sea water from the part of ships or (art. 137 DL. 152/06);
- Non-authorized waste management activities (art. 256 DL. 152/06);
- Pollution of soil, subsoil, surface water and groundwater (art. 257 DL. 152/06);
- Violation of the obligations of communication, of the obligatory keeping of books and of registers (art. 258 DL 152/06);
- Illicit waste trafficking (art. 259 DL. 152/06);
- False indications on the nature, on the composition and on the chemical-physical characteristics of waste upon the drafting of a waste analysis certificate; entering of a false waste analysis certificate in SISTRI, omission or fraudulent alteration of the paper copy of the SISTRI sheet - area waste transportation management (art. 260 *bis*, DL 152/06);
- Sanctions (art. 279 DL 152/06);
- Fraudulent pollution caused by ships (art. 8 DL. 202/07);
- Involuntary pollution caused by ships (art. 9 DL 202/07);
- Environmental Pollution (art. 452 *bis*, Penal Code);
- Environmental Disaster (art. 452 *quarter*, Penal Code);
- Involuntary crimes against the environment (art. 452 *quinquies*, Penal Code);
- Trafficking and abandoning of radioactive material (art. 452 *sexies*, Penal Code);
- Aggravating circumstances (art. 452 *octies*, Penal Code);

Crimes deriving from the employment of third-country citizens whose stay is irregular

- Employment of foreign workers without permit of stay or whose permit has expired or has not been renewed within the terms set by the Law. Employment of foreign workers whose permit of stay has been revoked or annulled (art. 22 c. 12 *bis*, DL. 286/98)
- Dispositions against clandestine immigration (art. 12 co. 3, 3 *bis*, 3 *ter*, 5 DL. 286/98)

Transnational Crimes

- Crime Association (art. 416 Penal Code);
- Mafia-style crime association (art. 416 *bis*, Penal Code);
- Instigation not to make statements or to make false statements to the Judicial Authority (art. 377 *bis*, Penal Code);
- Personal aiding and abetting (art. 378 Penal Code);
- Crime association aimed at the smuggling of foreign tobacco (art. 291 *quarter*, DPR 43/1973)
- Association with the purpose of illegal trafficking of drugs or psychotropic substances (art. 74 DPR 309/1990)
- Dispositions against clandestine immigrations (art. 12 par. 3, 3 *bis*, 3 *ter*. and DL. 25th July 1998, n. 286: "Single document of the dispositions concerning the discipline of immigration and rules on foreigners' conditions")

Racism and xenophobia

- International convention on the elimination of all forms of racial discrimination (art. 3 co. 3 *bis*. L. 654/75)

3. SANCTIONS

The sanctions to be applied to the Body for the administrative offences deriving from the committing of the crimes as per Decree Law. 231 are:

– *Monetary Sanctions (precautionary preventive seizure): they are based on the quota system.*

The amount of the quota must not be inferior to one hundred and not higher than one thousand. It is comprised between a minimum of Euros 258.23 and a maximum of Euros 1,549.37. In order to quantify the monetary sanction, the Judge shall determine the number of quotas with reference to the seriousness of the offence, to the Body's level of responsibility and the activities carried out. This is done both to eliminate/mitigate the consequences of the fact, and to prevent the committing of other crimes. The value of the amount is defined based on the Body's economic and assets conditions in order to assure the efficacy of the sanction.

– *Interdictory Sanctions (applicable also as preventive measures). They are:*

- Interdiction from the exercise of business activities;
- Suspension or withdrawal of authorisations or of licences functional to the committing of the crime;
- Prohibition of entering into an agreement with the Public Administration, except for obtaining the benefits of a public service;
- Exclusion from facilitations, financing, contributions or subsidies and the eventual revocation of the ones already granted;
- Ban on advertising goods or services.

Interdictory sanctions are applied with reference to the crimes for which they are expressly provided for, when at least one of the following conditions occurs:

- the Body has gained an important profit from the crime and the offence has been committed by Subjects in top positions, or by Subjects subordinate to somebody else's management, when the committing of the crime has been determined or made easier by serious organisational deficiencies;
 - in the event of the reiteration of offences. The reiteration exists when the Body has already been convicted for criminal offence in a definitive way at least once and it commits another crime in the 5 years following the final conviction.
- *Publication of the sentence: it can occur when an interdictory sanction is applied to the Body.*

The judgement is published only one time, wholly or partially, in one or more papers mentioned by the Judge in his/her judgement. The judgement is also put on display in the town/city where the Body has its headquarters. The publication of the judgement is carried out by the Registry of the Judge at the Body's expense.

– *Confiscation (or preventive cautionary confiscation): with the conviction judgement, the Body is always confiscated the price or the profits of the crime, to the exception of the part that can be returned to the damaged party.*

When it is not possible to carry out the indicated confiscation, amounts of money, goods or other benefits of equal in value to the price or the profit of the crime can be confiscated instead.

Only the Body is responsible for the obligation for the payment of the monetary sanction with its assets or funds. Business Partners and/or Members shall not be held responsible.

4. THE ORGANIZATION, MANAGEMENT AND CONTROL MODEL

4.1 Exempting value of the Model

Art. 6 of the Decree Law 231 states that the Body does not respond of the crime committed in its interest or advantage if:

- *it can demonstrate that, before the committing of the crime, the Body "adopted and efficaciously implemented organisation and management models (further qualified as "control" models in art 7 of the Decree Law 231) suitable for preventing crimes similar to the one that was committed";*
- it instituted an appropriate internal control body with the task of watching on the functioning, the efficacy and the observance of the afore-mentioned models. This internal Body is also to take care of updating the same models.

Such organization, management and control models are to comply with the following needs:

- identifying the activities at risk of committing the crimes provided for by Decree Law 231/2001;
- providing for specific protocols aimed at programming the training and the actuation of the Body's decision with reference to the crimes to be prevented;
- identifying the management modalities of the financial resources aimed at preventing the committing of such crimes;
- providing for information obligations towards the Body entrusted with supervising the functioning and the observance of the models (here below: "Supervisory Bodies");
- introducing a disciplinary system suitable for sanctioning the non-respect of the measures stated in the Model.

If the crime is committed by Subjects that have a Body's representative, administrative or managerial role or carry out the same tasks for a Body's organisational unit possessing financial and functional autonomy or, if the crime is committed by Subjects who effectively carry out the management and the control of the same (art. 6 DL. 231), it is necessary to point out that the Body "*is not held responsible, if it demonstrates*" that:

- before the committing of the offence, the Managing Body adopted and efficaciously implemented an appropriate Model aimed at preventing crimes similar to the one that was committed;
- the task of supervising the functioning and the observance of the Model and to look after its updating has been given to a Body's Entity in possession of autonomous powers of initiative and control;
- the Subjects have committed the crime fraudulently avoiding the Model;
- the Supervisory Body has appropriately and sufficiently watched on the application of the Model.

Instead, if the crime were committed by Subjects that are subordinate to the Management or to the supervision of one of the afore-mentioned Subjects (art. 7 of the afore-mentioned Decree), the Body shall be held responsible, if the committing of the crime was made possible by the non-observance of the management and supervisory obligations. In any case, such non-observance is excluded if the Body, before the committing of the crime, adopted and efficaciously implemented a Model aimed at preventing crimes similar to the one that was committed.

4.2 Exempting Eligibility of the Model

The Penal Judge is to ascertain the Body's responsibilities. In addition to the starting of an *ad hoc* trial in which the Body is equalised to the individual under investigation, the ascertaining process is carried out as follows:

- verification of the existence of the supposed crime that gives rise to the Body's liability; and
- the verification of the appropriateness of the adopted organisational models.

Thus, only when the Judge considers the Model appropriate for the prevention of crimes similar to the one that has been committed, the Exempting Eligibility of the Model shall be confirmed to the Body. As such, the Body shall not suffer the sanctions provided for by DL. 231/2001.

5. THE TRADE ASSOCIATIONS' GUIDELINES

The organisation, management and control Models can be adopted based on forms of behaviour expressed by the Bodies' Trade Associations and communicated to the Ministry of Justice. This guarantees what expressed by art. 6, chapter 2, of the DL 231.

Confindustria was among the first Associations to draft some Guidelines for the preparation of the Models. In march 2002 Confindustria issued some Guidelines, subsequently partially modified and updated.

This Model was based on Confindustria's Guidelines. The Ministry of Justice has judged all the mentioned versions of Confindustria's Guidelines adequate for the reaching of their objectives. As such, they were used as a point of reference upon the drafting of this Model.

GENERAL PART

6. ECOPNEUS' ORGANISATION, MANAGEMENT AND CONTROL MODEL

6.1 Aim and contents

The organisation, management and control Model is a complex body of principles, rules, dispositions and organisational schemes with the objective of creating and diligently applying a control and monitoring system of the sensitive activities. This aims at preventing the (even attempted) committing of the crimes provided for DL 231. The preventive aim of the Model is applicable to Subjects in senior positions, and to Subjects depending on somebody else's management and operating on behalf of Ecopneus ("EP").

Thus, the Model wants to configure an organic and structured system of procedures and control activities aimed at preventing and reducing the risk of committing the crimes as per DL. 231/2001.

The identification of the activities at risk of crime committing and their subsequent formalisation in procedures in an efficacious system is to:

- make sure that all those who act in the name and on behalf of EP are fully aware of the risks and sanctions the Company would face in case of crime committing;
- allow EP to promptly adopt the most appropriate measures and precautions to prevent the committing of crimes.

Among the aims of the Model there is, thus, the one of making sure that Employees, Company Bodies, Consultants and Partners operating on behalf of and/or in the interest of EP with reference to sensitive processes understand the great importance of respecting roles, operative modalities, Company's rules, regulations and internal procedures. In other words, they are to fully understand the importance of implementing the organisational model. They are also to be aware of the corporate value of such Model in order to prevent crimes.

The Model is approved by EP's Board of Directors.

6.1.2 Improvement of governance rules

The adoption and valid implementation of the Organisation Model (and of all rules, procedures, principles, and protocols mentioned in the Model that are integrating part of the same) allow the Company to benefit from the legitimate expectation of the exemption as per art. 6 of the Decree Law 231/2001. It also allows the Company to be able to develop and improve its own management and administration rules. Indeed, even in consideration of the importance of EP's role as per DL. 152/2006 art. 228, the Company wants to assure as much management transparency and regularity as possible. This is to happen in compliance with all Legislation, and avoiding whatever illicit form of behaviour that is against the rules.

6.2 Recipients

This model is applicable in all EP's offices, Areas, Division and Functions.

All those who work for the achieving of EP's corporate aims and objectives are the recipients of this document.

Recipients of this Model are: the members of EP's Corporate Bodies, the Subjects involved in the Supervisory Body Functions, the Employees and, in general, all Third Parties directly or indirectly acting to the advantage of EP. Examples of third-party Subjects are:

- those who have a non-subordinate working contract with the Company (e.g.: Contract Workers, Consultants, Temporary Workers);
- All types of Collaborators and Consultants;
- Attorneys, Agents, and all those people who act in the name and/or on behalf of the Company;
- Suppliers and eventual Partners.

6.3 Methodological Principles and Guiding Principles

6.3.1 Identification of sensitive Areas, Activities and Processes (the so-called: “As is Analysis”)

The afore-mentioned Guidelines specify that *the steps made for the construction of the Model facilitate the application of the exemption*.

For this reason, here-below it is highlighted the identification of the risks and of the planning of the control system which has led to the creation and the subsequent updating of this Model. Further documentation is filed at the Company.

Among the organisation and management Models, art. 6, par. 2, lett. a) of the DL 231 indicates the identification of the so-called “sensitive areas” or areas at “risk”. They are those processes and corporate activities where there may be a risk of committing one or more of the crimes as per the afore-mentioned Decree Law.

The Company has carried out an in-depth analysis of its reality. This analysis is constantly updated by the means of the analysis of the available corporate documentation (legislation of reference, organisational chart, governance system, overall system of delegated powers and proxies, internal policies and procedures etc.). It is also updated by the means of a number of interviews with the Managers or key-subjects of the Company’s structure.

Moreover, the existing operative and management modalities and the effectively governing control elements have been identified for each sensitive area and process.

The analysis of corporate processes is carried out in the afore-described forms and ways. It has allowed to identify those critical areas where the committing of the crimes provided for by DL 231 may happen. (the so-called: *risk mapping*).

6.3.2 Risk Assessment, Gap Analysis, Action Plan

In order to identify and carefully analyse the existing control system governing the identified risks which have been highlighted in the risk assessment activity, a gap analysis is carried out between the organisational system and the system of the existing controls (“as is”) and the model of reference currently defined as per the same DL 231 (“to be”). A gap analysis is also made in order to evaluate the capacity of the same system to comply with the requisites set by DL 231.

It is possible to identify the existing internal control system improvement areas, through the comparison carried out with the gap analysis. Based on the results, an action plan is drafted aimed at:

- (I). identifying the improvement and updating actions of the existing corporate procedures which are part of the internal control system and the organisational requisites essential for the definition and realisation of an organisation, management and control Model. The latter is to comply with what stated by DL. 231 and it should reduce the identified risks to an acceptable level;
- (II). Defining protocols, Company’s rules and control and management procedures.

6.3.3 Risk Analysis Results

In the evaluation of the relevant risks as per DL. 231/2001, an examination of the single type of crimes or of groups of crimes sharing the same juridical asset was made. This highlighted the eventual existence of sensitive areas (including sensitive activities and processes) for every sector examined.

The results have been filed in the Company. They have allowed to identify the following areas at risk and to prepare the related Special Parts:

- Areas at risk for Crimes against the Public Administration
- Areas at risk for Corporate Crime
- Areas at risk for crimes of Manslaughter and very serious injuries for the violation of the rules for workers’ health and safety
- Areas at risk of IT crimes and illicit Data Management
- Areas at risk of Organised Crime Offences
- Areas at risk of Crimes of receiving of stolen goods, of money-laundering, and of use of money, goods and benefits of illicit provenance, as well as crimes of “self-laundering”
- Areas at risk of crimes against industry and commerce
- Areas at risk of crimes of Instigation not to make statements or to make false statements to the Judicial Authority
- Areas at risk for Environmental Crime

The identified areas at risk are detailed in the Special Parts as indicated here-below.

6.3.4 Model Preparation

Thus, this document takes into consideration:

- Confindustria's Guidelines
- The requisites stated by the DL 231 and, in particular:
 - Giving a Supervisory Body the task of promoting an efficacious and correct application of the Model. This shall be done also by the means of the monitoring of corporate behaviour and the right to constant information on the activities relevant to the aims of the Decree;
 - The awarding of resources to the Supervisory Body (even in terms of power expenditure) adequate for supporting it in the execution of its tasks and for the reaching of reasonably attainable results;
 - The activity of verification of the functioning of the Model with its subsequent periodic update (*ex post* control);
 - The activity of awareness raising and diffusion, at all company's levels, of all behavioural rules and the instituted procedures;
- The general principles of an adequate internal control system and, in particular:
 - The verifiability and accountability of each operation relevant to the aims of the Decree;
 - The respect of the Principle of the Separation of Functions. According to this principle, nobody can autonomously manage a whole process (to the exception of those cases in which it is necessary to do so, because of the peculiarity of the activities or of the essentiality of the organic plan);
 - The definition of powers of authorisation that are coherent with the entrusted tasks, as well as the objectification of the decision-making processes. This shall allow to make sure that decisions are taken regardless of merely subjective evaluations;
 - The communication of relevant information to the Supervisory Body;
- the National Category Contract applicable to the Company;
- the Italian applicable Laws (such as: Law 300/1970 – Workers' Statute of Rights, Decree Law 81/2008 – Single Text on Safety on the Workplace, Decree Law 196/2003 – Code on Privacy, the Rules recalled by Decree Law 231/2001, etc.).
- Moreover, upon drafting this document, corporate rules were taken into consideration, as well as the procedures and the existing regulations, if deemed appropriate (and eventually integrated) as precautionary measures for preventing crimes and as ways of controlling sensitive processes.

6.4 Model Modifications

EP's Board of Director is responsible for the approval of every modification of the Model. In particular, such modifications may be appropriate in case of:

- organisational modifications or changings in corporate activities;
- adoption, adaptation, integration, suppression of corporate rules and/or procedures;
- extension of the list of offences provided for by the Decree or other modifications of the Law;
- discovery of violations of the provisions.

6.5 EP's Organisation

6.5.1 Organisational Chart

The analysis of the Company's organisational charts highlights a fairly simple, but highly specialised, organisational structure. It is based on the clear hierarchic identification of the Subjects operating for the Company.

The President of the Board of Directors is the Head of the Company. He/she is followed by the General Manager, who acts also in his/her role of Employer as per Decree Law 81/2008.

It is here specified that, based on the Shareholders' Agreements, the Presidency of the Board of Directors is held by each member based on an annual rotation system.

The General Manager reports to the BoD and to the President; the People Responsible for the Areas (Administration and Personnel; Operations and Logistics, Development of Uses and Rules; District Oversight; IT Systems) report to the General Manager. The rest of the Employees are in a subordinate position.

The judicial services, the services of purchasing, communication and call centre are not directly managed by the Company, but they are provided for by external companies and professionals.

6.6 The principles that have inspired corporate rules and procedures (control system)

Corporate rules and operative procedures for each risk area are inspired by a general preventive control system. They obey fundamental principles among which are the following:

- "Every operation, transaction, action is to be: verifiable, documented, coherent and congruous".

All operations, in particular those related to financial management, are, thus, to be justified and justifiable by the means of appropriate documental support. This allows a prompt control of the decision, of the authorisation, of the modalities of execution and of the verifications of the same operation.

– “Nobody can autonomously manage a whole process” (to the exception of those cases in which it is necessary to do so because of the peculiarity of the activities or of the essentiality of the organic plan);

Such principle is aimed at guaranteeing the separation of the functions, in order to assure that the authorisation of the execution of an operation falls within the responsibility of a Subject that is not the one who accounts it, or the one who operatively executes or verifies it.

The corollary of such principle is the structuring of Company’s organisation in a way that makes sure that the relative powers and fields of operations and responsibility are predefined, coherent, known, and shared.

In particular, in the financial management area, the accounting procedures are to guarantee the respect of the principles of transparency, verifiability and inherence to Company’s activities. This is to be done also by the means of the adoption of operative procedures such as: the contraposition of the purchasing Function to the Financial Function, the supervision of operations, the reconciliation of the accounts and final checks.

The signatory powers are correlatively awarded coherently with the predefined corporate responsibility, providing for, in particular, the indication of the thresholds for the expenditure approval.

Thus, the most relevant elements of the control system, which shall be explicated in the single Special Parts, are:

- Code of Ethics;
- Organisational System;
- Company’s Rules and Regulations;
- Procedures;
- Powers of authorisation and signatory powers;
- Control Systems and Technical Auditing;
- Communication to Members of Staff and their Training;
- Provision for an adequate sanctioning system for the violation of the rules of the Code of Ethics and of the procedures provided for by the Model;
- Obligations of notification to the Supervisory Body.

The control system put into place by the Company is conceived in a way that guarantees that the same control system cannot be circumvented, if not fraudulently.

6.7 Procedures, Company’s Rules and other internal Documentation

The management and distribution of the documentation is done in a controlled way by the means of the Company’s network or in paper copy.

Within the afore-mentioned Areas or Functions, the activities follow a procedure based on consolidated corporate practices, operative protocols, and Company’s rules communicated and put at disposal of EP’s Employees.

In addition to the Code of Ethics, to the Administrators’ Self-Discipline Code, to the Risk Evaluation Document (as per DL 81/2008), and to the Safety Planning Document (DPS- as per DL 196/2003), the Company adopts a number of regulatory rules and procedures, in particular in purchasing, in the selection of Suppliers, in the management of financial resources, in the payment systems, and in the management of the expense sheets.

Within the scope of financial flows management, and in order to monitor the incoming and outgoing flows, the Company uses the SAP IT management system.

With reference to the management of economic and financial data that make reference to the ELT management chain, the same are managed by the means of the software “Eltis”.

Company’s rules are usually issued by the General Manager in his/her role as Employer as per DL. 81/2008 and due to the fact that they may become effective as per the Model ex DL. 231/2001. Company’s rules are approved by the Board of Directors together with the Model, as they are integrating part of the same.

6.8 Code of Ethics

The Company has adopted its own Code of Ethics, based on uniform behavioural principles. The Code of Ethics is to be adopted by all Company’s Bodies, Managers, Employees and Collaborators during the carrying out of their working activities, both with reference to the inter-company relationship, and with reference to their relationship with Third Parties. The violation of the Code implies the possible application of a number of sanctions provided for by the Disciplinary System, as per the here-below Chapter 8.

Upon the carrying out of its own activities, EP requires a rigorous behavioural standard based on the principles of honesty, transparency, ethical correctness and loyalty in the execution of commercial operations, and in Company’s relationship with Third Parties.

In particular, the Code dedicates a specific Function to the sanctioning of forms of discriminatory behaviour on the workplace. It also states the most appropriate forms of conduct aimed at avoiding possible critical situations. Further paragraphs are dedicated to environmental protection and Company's policies with reference to safety, health and the wellbeing of its Employees. This is done by providing for the active promotion of the safety measures and prevention of accidents on the workplace.

Another sector of the Code deals with possible conflicts of interest. It expressly states that EP's Employees are to rigorously refrain from accepting compensation, loans, or gifts different from the habitual ones offered by Third Parties in connection with any commercial transaction. Moreover, all Employees are to immediately inform the Company about possible conflicts of interest that may involve the Employee or his/her relatives, directly or indirectly, and that are inherent to the prohibition of non-competition.

Moreover, the Code provides for the creation of a communication channel by the means of which the Employees can report episodes of violation of the same Code.

The Code of Ethics is here fully referred. It summarises all the values that are always to be adopted by all EP's organisation and that can be summarised as: "*our values, always.*"

What here-above shows that the Model and the Code of Ethics are two separate documents with different objectives, even if they integrate one another to create a body of rules that increment corporate ethical culture. The Model complies with specific rules expressed in DL 231/2001 aimed at preventing the committing of certain types of offences. The Code is an autonomous general tool with the goal of promoting the Company's Code of Ethics.

7. SUPERVISORY BODY'S ARTICLES OF ASSOCIATION

7.1 Identification and operating requisites

In order for the Company not to be held liable for the committing of the serious crimes listed in DL 231, it is necessary to create a Supervisory Body (SB). This SB is to be "*in possession of autonomous powers of initiative and control*" and it has the task of "*watching on the functioning and the observance of the Model, taking care of its updating*" (art. 6 aforementioned Decree).

The SB is a corporate Body. It is autonomous and independent from the other Bodies, in particular, with reference to the executive ones.

The requisites the SB is to satisfy for the effective performance of the afore-mentioned functions are:

- Autonomy and Independence. The Supervisory Body must not have operative tasks. It is only to relate with the Company's operative Top Management (Administrative Body and General Manager). Thus, it is necessary for the SB to have an autonomous control power (appropriate for the execution of the Function of vigilance and the observance of the Model) and an autonomous power of initiative to guarantee the updating of the Model;
- Professionalism in carrying out its institutional tasks. The members of the Supervisory Body are to have specific knowledge about the techniques useful for preventing the committing of crimes, for discovering the already committed offences, for identifying their causes and for verifying that corporate organisation Members comply with the Model;
- Continuity of action. Among the other things, such requisite implies the periodic presence of the Supervisory Body in the Company without access limitations.

From the moment that there is no structure within EP in possession of the afore-described requisites, it was necessary to create an appropriate Body *ex novo*.

The members of the SB can be chosen among Subjects that are internal or external to the Company. In any case, the members of the SB are to be qualified and experts in the relevant subjects to the aims of DL 231/2001, especially with reference to corporate Law and risk assessment. They are also to have significant experience as SB's members and they are also to possess the requisites of professionalism and respectability.

According to the best practice, Ecopneus Scpa's Board of Directors decided to create a Supervisory Body composed of two external members. This is to highlight the dialectic and the independence of the Function. That is:

- the SB's members must not have commercial relationships with the Company that may imply potential conflicts of interest with reference to the Supervisory Body's areas of competence;
- the SB's members must not be relatives of Partners or Administrators, as this may imply a reduction of their judgemental autonomy;
- the SB's members must not be connected in any possible way or for whatever reason to the Company; they must not be dependent on the Company or subordinate to the same;

The Supervisory Body's members nominate a President.

7.2 Functions and Powers

Based on what it is possible to evince from the text of the DL 231/2001, the Functions carried out by the Supervisory Body can be schematised as follows:

- Vigilance on the Model effectivity. This consists of verifying the coherence between the concrete forms of behaviour and the instituted Model;
- Evaluation of the Model adequacy and of the appropriateness of the same, with reference to the typology of activities and the characteristics of the enterprise, in order to prevent the committing of the crimes as per DL. 231.
- Model updating based on the evolution of Company's structure and on changing of legal provisions.

From an operative point of view, the Supervisory Body is entrusted with the following tasks:

- verifying that the organisational, management and control protocols defined in the Model are effectively applied;
- periodic mapping of Company's procedures related to the areas of the activities at risk;
- periodical carrying out of checks of specific operations within the scope of corporate activities at risk;
- collecting, elaborating and filing of the information coming from the different corporate Functions with reference to the respect of the Model;
- taking care of the spreading of Model knowledge and understanding;
- controlling the relationship with Third-Party Subjects with reference to the aims of the Model;
- collecting, keeping and evaluating the notifications of eventual Model violations;
- coordinating the relationships with the Company's Functions involved in the relevant processes and with the Board of Auditors, in order to activate an efficacious vigilance activity for the respect of the rules and for the effective application of the Model;
- carrying out internal investigations following the notifications of eventual violations of this Model, if considered serious and harmful for the Company. Expressing non-binding opinions on the typology and the severity of the sanction.

Upon carrying out its tasks, the Supervisory Body:

- acts in full autonomy and its activities cannot be questioned by any other Company's Body or structure;
- has unlimited access to Company's information for the activities of investigation, analysis and control;
- must be financially and logistically independent in order to guarantee its full operation. To this aim, when drafting the budget, the Board of Directors provides for the awarding of an adequate fund of €20,000.00 to the Supervisory Body upon request of the same. This fund can be used for the expenses incurred by the Body in the carrying out of its functions, there included the assigning of eventual consultancy services. The Supervisory Body is to supply appropriate justification for any expense incurred. Within the limits of the moneys awarded by the Board of Directors, the Supervisory Body has control of its resources autonomously and directly. This is an exception to the normal procedures of financial and administrative management existing within the Company for the other corporate structures;
- has the faculty of asking for and/or entrusting third-party Subjects to carry out tasks of technical nature. These Third-Party Subjects are to possess the necessary specific competences for the execution of their tasks at their best;
- has the right to request the support of all Company's Functions.

7.3 Appointment, Termination, Ineligibility and Revocation

The Supervisory Body is created with the decision of the Board of Directors.

The duration of the mandate is of two years and it can be renewed for periods of the same duration. In any case, the SB decayed for expiry of its mandate stays in charge until its substitution and/or confirmation.

After listening to the Board of Auditors' opinion, the Board of Directors can start an action of withdrawal of the mandate of the Supervisory Body. Necessary and sufficient motivation for the withdrawal is the documented non-compliance of the Subject in carrying out the activities and responsibility deriving from the mandate.

Causes of the ineligibility and/or revocation of the Supervisory Body are:

- the final judgement for committing one of the crimes provided for by DL. 231; or
- the final judgement for an offence that implies a (even temporary) ban from holding public offices, or the temporary ban from management offices of legal persons and companies.

In particularly serious cases, even before judgement and after listening to the Board of Auditors' opinion, the Board of Directors can order the suspension of the Supervisory Body's powers and the nomination of an interim body.

7.4 Information flows and notifications to the Supervisory Board

All Company's Functions are to notify the Supervisory Board about any piece of information related to the application of the Model. The information may come also from Third Parties.

In general, the members of the Board of Directors, the members of the Board of Statutory Auditors, the Employees and all those Subjects who are entrusted with professional tasks by the Company are obliged to inform the Supervisory Body. Such information obligation is applied to any piece of news related to the committing of crimes, to forms of behaviour that do not comply with the procedures, and to the rules of conduct provided for by the Model and the Code

of Ethics. It also makes reference to any eventual fault of the organisational structure or of Company's procedures and rules in force. The violation of this information obligation constitutes a disciplinary offence based on what stated by the Model, by the Law and by the applicable collective contracts.

The following general rules apply:

- any eventual notification of the committing (or the reasonable risk of committing) of a crime listed in DL 231 is to be collected by each person in charge. The same procedure applies for those offences related to forms of behaviour that do not comply with the behavioural rules as per the Model;
- each Employee is to notify the violation (or supposed violation) of the Model by contacting the Supervisory Body;
- for what concerns the activities they carry out to the advantage of EP, the Consultants, Collaborators and Business Partners are to directly notify the Supervisory Body by the means of the modalities stated in their contracts.

The Supervisory Body evaluates the received notifications and the activities to be implemented. The eventual measures deriving from the notifications are defined and applied in agreement with what provided for by the Disciplinary System. The people reporting facts in good faith are protected from all forms of retaliation, discrimination or penalisation. In any case, the confidentiality of the identity of the person reporting the crime shall be assured, unless otherwise provided for by the Law and the protection of Company's rights or the protection of the people erroneously accused or accused in bad faith.

In addition to the notifications related to violations of general nature as described here-above, the Supervisory Body is to be informed about all disciplinary measures put into place with reference to the notification of violation of the Model and to the sanctions imposed (there included the measures taken towards the Employees). The SB is also to be informed about the procedures for the filing of such measures with their related motivations.

The notifications are to be sent directly to the Supervisory Body, by the means of written communication to:

OP's Supervisory Body, e-mail: Odv231@ecopneus.it.

In order to guarantee the confidentiality of the identity of the person reporting the offence, the notifications to the Supervisory Body can be made also anonymously, providing they are adequately detailed, by the means of a letter addressed to:

EP's Supervisory Body, address: Via Messina, n. 38 Milano (MI) 20154

In this case, the Supervisory Body will evaluate the appropriateness and reliability of the notification before going ahead with the appropriate investigations.

7.5 Reporting to Company's Bodies

The Supervisory Body reports on the state of application of the Model and on its activities according to the following modalities:

- orally and constantly to the President and/or to the General Manager. These shall inform the Board of Directors within the scope of their respective mandates;
- annually and in writing to the Board of Directors (to the attention of its President) and to the Board of Statutory Auditors (to the attention of its President);

To this aim, the Supervisory Body prepares an annual report about to its activities (the control and specific verifications carried out and the results of the same; the criticalities; the eventual updating of the mapping of sensitive processes etc.). The report is also about the legislative innovations with reference to Bodies' administrative responsibility.

The Supervisory Body can be summoned in any moment by the afore-mentioned Bodies. In its turn, it can make a request of being summoned, in order to report about the functioning of the Model.

Moreover, it is expected that:

- upon notification of a violation of the Model committed by one or more of Board of Directors' Members, the Supervisory Body informs the Board of Statutory Auditors and the Administrators;
- upon notification of a violation of the Model committed by one or more of the Statutory Auditors, the Supervisory Body shall inform the Auditors and the Board of Directors.

7.6 Supervisory Body's Meetings, Collection and Filing of Documentation

The Body periodically carries out all necessary activities for the execution of its functions.

The Board of Directors and the Board of Statutory Auditors can summon the Body at any time.

The meetings are recorded, signed and kept by the Body in its own archives.

During the carrying out of inspective checks at the Company's offices, the Body can decide to go ahead with interviews of Company's Employees, Members of Company's Bodies and external Consultants.

Such interviews can be recorded.

The Body can discipline the aspects related to the carrying out of its activities (determination of control deadlines, identification of the analysis criteria and procedures etc.) by the means of internal Rules of its own.

All documentation related to the Model, such as: information, notifications, reports etc., are kept by the Supervisory Body in a specific IT and/or paper archive.

7.7 Confidentiality

The Supervisory Body, the components of Company's technical structures, and the external Consultants the Body may eventually avail itself of are bound by the requirement of confidentiality with reference to pieces of news and information obtained during the course of the execution of their functions, without prejudice to the obligations of information expressly provided for by the Law and/or by this Model. Moreover, it is assured that the afore-mentioned pieces of news and information are used exclusively for the aims stated by art. 6 of the Decree. In any case, every piece of information in possession of the Body's Members, of the Members of the Company's technical structures and of the external Consultants is dealt with in compliance with the legislation in force and, in particular, in compliance with the Single Text about Data Protection, DL 30th June 2003, n. 196.

7.8 Compensation

The Board of Directors sets the compensation for the activities of the Supervisory Body's members upon their appointment.

7.9 Modifications

Any eventual modification to this Document can be made exclusively by the Board of Directors after listening to the opinion of the Supervisory Board and of the Board of Statutory Auditors, either on their own initiative or on the Supervisory Body's initiative.

8. DISCIPLINARY SYSTEM

8.1 Function of the Disciplinary System

Art. 6, par. 2, lett. e) and art. 7, par. 4, lett. b) of the DL. 231/2001 establish (with reference both to Top Management and to Employees in subordinate position) the necessary preparation of *"an appropriate disciplinary system for sanctioning the non-respect of the measures described in the Model"*.

The sanctions are commensurate to the violation. They are in possession of deterrent measures and are applicable in case of violation of the measures described in the Model and in the Code of Ethics. The definition of sanctions has the aim of contributing: (i) to the efficacy of the same Model and (ii) to the efficacy of the Supervisory Body's control actions. The application of the disciplinary system is independent from the carrying out and the results of the criminal proceedings eventually started by the Judicial Authority of competence.

The Violation of the Rules of the Model and of the Code of Ethics constitutes a breach of the relationship of trust with the Company. It integrates a disciplinary offence that can be sanctioned.

The Disciplinary System is applied in compliance with the legislation in force, there included (where applicable) the rules provided for by collective contracts. It is internal to the Company, from the moment that it intends adding further obligations compared to the ones provided for by the Law or by the Rules in force.

The Disciplinary System is located within the Company's offices, in a place open to everybody, in order to guarantee the full knowledge of the same from the part of all the Recipients here-below identified.

8.2 Relevant Types of Conduct

The actions (even omitting ones) and the forms of behaviour violating EP's organisational Model are forms of conduct that can be sanctioned.

With "violations of the Model" it is meant also the violations of the prohibitions, protocols, and Company's rules that are integrating part thereof, and also the violations of the Code of Ethics.

The forms of behaviour (there included the omitting ones) that violate the Supervisory Body's indications and/or prescriptions are also considered violations of the Model.

Subject of the sanctions are the violations of the Model made by Top Management, as Senior Managers are entrusted with powers of representation, administration and management of the Body. In other words: they are *de facto* entrusted with the Body's management and control powers. Subject to sanctions are also the violations committed by people subject to somebody else's management or control or, in any case, operating in the name and on behalf of the Company.

8.3 General Criteria for the imposition of Sanctions and/or Protection Measures

In every single case, the type and entity of the specific sanctions will be applied in proportion to the gravity of the infringement and, in any case, based on the following general criteria:

- subjective element of conduct (fraud or fault. The latter for negligence, imprudence or lack of competence);
- relevance of infringement of obligations;

- potentiality of the damage deriving to the Company or from the eventual application of the sanctions provided for by DL. 231/01;
- level of hierarchic or technical responsibility;
- presence of aggravating or attenuating circumstances, bearing particular attention to the precedent working performances and to the disciplinary history of the previous two years;
- eventual responsibility shared with other workers who may have concurred in the infringement.

If a single act were to cause more infringements punishable with different sanctions, the hardest punishment shall be applied.

The recurrence of the offence in the two-year period automatically implies the application of the hardest form of punishment within the typology provided for.

8.4 Communication of Violations and Sanctioning Procedure

The procedure of enforcement of sanctions and/or of the protection measures will start after the Supervisory Body has communicated the effective violation of the Model to the Company's Bodies of competence.

Indeed, the SB is obliged to activate itself in order to carry out all checks and control falling within the scope of its activity of vigilance and verification – elements that may cause the danger of violation of the Model.

Once the activities of verification and control have finished, the SB is to evaluate if the violation of the Model has effectively happened. In that were the case, the SB shall notify the violation to the Company's Bodies of competence.

In particular, if the Supervisory Body were to find a form of behaviour to be sanctioned after its verifications:

- with reference to Senior Managers, Middle Managers and Employees: the SB is to promptly inform the General Manager;
- with reference to Administrators, and the General Manager: the SB is to promptly inform the President of the Board of Directors and the President of the Board of Statutory Auditors;
- with reference to the President of the Board of Directors: the SB is to promptly inform the other Administrators and the President of the Board of Statutory Auditors;
- with reference to the effective Statutory Auditors: the SB is to promptly inform the President of the Board of Directors and the President of the Board of Statutory Auditors;
- with reference to the President of the Board of Statutory Auditors: the SB is to promptly inform the other Statutory Auditors and the President of the Board of Directors;
- with reference to external Collaborators: the SB is to promptly inform the General Manager.

The General Manager issues the sanctions towards the person who committed the offence for the categories of Senior Managers, Middle Managers, Employees and external Collaborators. The disciplinary sanctions and/or the protection measures towards the Administrators, the Statutory Auditors and the General Manager are decided by the Board of Directors and/or the Assembly. The sanctions and/or the protection measures towards the President of the Board of Directors and the President of the Board of Statutory Auditors are decided by the Board of Directors together with the Board of Statutory Auditors and/or the Shareholders' Meeting.

The sanctioning procedure takes into consideration:

- the rules of the Civil Code about corporate, labour and contractual matters;
- the labour legislation about disciplinary sanctions as per art. 7 Law n. 300 – Workers' Statute;
- Company's Articles of Associations;
- the current powers of representation, the powers of corporate digital signature and of the functions attributed to corporate structure;
- the necessary distinction and contraposition of the roles of the judging subject and the judged one.

Those who issue the sanctions are to inform the Supervisory Body by the means of a documented copy of the procedure.

The Management and the Supervisory Body verify the effective implementation of the applied sanction.

8.5 Sanctioning of Middle Management and Employees

8.5.1 Field of application

Without prejudice to the preventive contestation and the procedure provided for by art. 7 of the Law 20th May 1970 n. 300 (the so-called Workers' Statute), and according to what provided for by the current National Contract of the Rubber and Plastics Sector, the Company's Middle Management and Employees can be sanctioned in the following cases, as per art. 7 of the Decree Law 231/2001:

- non-compliance with the procedures and obligations of the Model aimed at guaranteeing the carrying out of the activities in compliance with the Law. These procedures and obligations are also aimed at finding out and promptly eliminate situations of risk;
- absence, incomplete or false documentation about the carried out activities; storage and control of acts concerning the procedures, in order to prevent the transparency and the verifiability of the same;
- violation and/or circumvention of the internal control system by the means of stealing, of the destruction or alteration of the documentation of the procedure; that is, preventing the control or the access to the information and the documentation to the Subjects in charge, there included the Supervisory Body;
- non-observance of the rules of the Code of Ethics;
- non-observance of the rules with reference to the signatory powers and of the system of the attributed delegations, above all of the requirements related to the matching modalities;
- non-observance of the obligation of informing the Supervisory Body and/or one's direct line manager about incorrect and/or anomalous and/or irregular forms of behaviour one directly knows about, with reference to violations of the Model and of the Code of Ethics;
- Senior Management's omitted vigilance on the compliance with procedures and requirements of the Model from the part of their own subordinates in order to verify their actions within the scope of the areas at risk of crimes and, in any case, during the carrying out of instrumental activities for operative processes at risk of offence;
- failure to train and/or update and/or omitted communication of the procedures and regulations of the Model to the Members of Staff subject to someone's management or vigilance and operating in the areas at risk of crime committing.

8.5.2. Sanctions

As a consequence of the violations as per the previous paragraph, EP's Middle Management and Employees are sanctioned with the following disciplinary procedures:

- verbal warning;
- written warning;
- fine not higher than three hours of retribution;
- suspension from work and from retribution for a period of up to three days;
- dismissal for non-compliance (without notice period but with Severance Pay).

If the afore-described employees are entrusted with the power of representing the Company, the imposing of a sanction worse than a fine shall imply also the automatic revocation of the same power.

Verbal warning

The following is punished with verbal warning:

- the negligent infringement of the principles of the Code of Ethics and/or of the procedures and requirements provided for by the Model;
- the repetition of forms of behaviour as per the previous point, when these forms of behaviour have external relevance;
- the carrying out of procedural mistakes cause by worker's negligence.

Written warning

The following is punished with written warning:

- the repetition of negligent infringement of the principles of the Code of Ethics and/or of the procedures and requirements provided for by the Model, when these violations have external relevance;
- the repetition of procedural mistakes caused by worker's negligence.

Fines

The following is punished with a fine:

- the repetition of the committing of infringements whence the application of written warning may come;
- negligent forms of behaviour that may undermine, even if only potentially, the efficacy of the Model bearing in mind the Subject's hierarchical or technical level of responsibility, or in the presence of eventual aggravating circumstances, such as, by way of example:
 - i) the non-observance of the obligation of informing the Supervisory Body and/or one's own line manager about anomalous or incorrect forms of behaviour a worker may have direct knowledge of;
 - ii) the repeated non-observance of the procedures and requirements described in the Model, if they make reference to a procedure where the Public Administration is involved.

Suspension from work and from retribution

The following is punished with the suspension from work and from the retribution for a period of up to three days:

- the repetition of the committing of infringements whence the application of a fine may derive;
- serious violation of procedures and requirements that may expose the Company to forms of liability towards Third Parties.

By way of example: the sanction of the suspension from work and from retribution is applied in case of:

- non-observance of the dispositions related to signatory powers; non-observance of the system of delegations attributed with reference to acts and documents addressed to the Public Administration;
- signalling related to violations of the Model and/or of the Code of Ethics, being aware of the falseness and baselessness of the same.

Dismissal for non-compliance

The sanction of dismissal is applied to those failings which are so serious that do not allow the prosecution of the work relationship, not even temporarily. Examples may be:

- intentional violation of procedures and requirements of the Model having external relevance, and/or fraudulent elusion carried out by the means of forms of behaviour unequivocally aimed at the committing of a crime provided for by DL. 231/2001, such as to interrupt the Employer's relationship of trust;
- violation and/or circumvention of the internal control system through the stealing, the destruction or the alteration of the documentation of the procedure, or preventing the control or the access to the information and the documentation to the Subjects in charge of verifications, there included the Supervisory Body, in order to prevent the transparency and verifiability of the same.

If the worker incurred in one of the failings as per this article, the Company may decide to go ahead with an immediate administrative leave, until the moment of the disciplinary action.

8.6 Sanctioning of Senior Management

8.6.1 Field of application

As per art. 7 of the Decree Law 231/2001, in compliance with the procedure provided for by art. 7 of the Law 20th May 1970 n. 300, and according to what stated by the current Senior Managers' National Contract, the Company's Senior Managers can be sanctioned in case of:

- non-compliance with the procedures and requirements of the Model aimed at guaranteeing the carrying out of the activities in compliance with the legislation, as well as promptly identifying and eradicating risk situations as per DL 231/2001;
- missing, incomplete or false documentation of the activities carried out with reference to the modalities of documenting, saving and controlling of the acts related to the procedures, in order to prevent the transparency and verifiability of the same;
- violation and/or avoidance of the internal control system. This could be done by the means of the stealing, of the destruction or of the alteration of the documentation of the procedure, or by preventing the Subjects in charge of verifications from controlling or accessing the information and the other documentation, there included the Supervisory Body;
- non-observance of the rules of the Code of Ethics;
- non-observance of the dispositions related to the signatory powers and of the system of the attributed proxies (above all the requirements related to the modalities of matching);
- non-observance of the obligation of informing the Supervisory Body and/or one's direct line manager about incorrect and/or anomalous and/or irregular forms of behaviour a Manager may have direct knowledge of, as well as false and ungrounded signalling, without prejudice of the good faith, related to the violations of the Model and the Code of Ethics;
- omitted supervision, control and vigilance of the behaviour of one's own subordinates, in order to verify their actions within the scope of the areas at risk of crime;
- omitted communication to one's line manager and/or to the Supervisory Body about the non-compliance with the procedures and requirements of the Model from the part of functionally assigned Subjects;
- failure to train and/or failure to update and/or omitted communication to the members of Staff working under them in the areas at risk of crime about the procedures and requirements of the Model.

8.6.2 Sanctions

As a consequence of the violations as per the previous paragraph and in consideration of the particular trust-based nature of their work relationship, the Company's Senior Managers are sanctioned with the following disciplinary measures:

- written reprimand;

– dismissal without notice period but with Severance Pay.

If the Senior Managers are entrusted with the power of representing the Company, the imposing of a written reprimand may imply also the revocation of the same power.

In order to identify the sanction to apply, the circumstance that the Manager, given the function or the position held, acts in the role of General Manager shall be considered as an aggravating factor.

Written reprimand

The written reprimand shall be issued in case of involuntary violation of procedural rules provided for by the Model or in case of procedural mistakes due to the Manager's negligence.

Dismissal without notice period

The Dismissal without notice period shall be issued when the relationship of trust between the Company and the Manager is irretrievably damaged and this would not allow the (even temporary) prosecution of the work relationship. Examples may be:

- the deliberate or involuntary violation of procedures with external relevance and/or their fraudulent circumvention by the means of forms of behaviour unequivocally aimed at committing one of the offences provided for by DL 231/2001 and its further modifications, as to irretrievably damage the relationship of trust with the Employer;
- violation and/or deliberate or involuntary circumvention of the control system. Such violations and/or circumventions may occur by preventing the Subjects in charge of verifications from controlling or accessing the information and the other documentation, there included the Supervisory Body;
- missing, incomplete or false documentation of the activities carried out with reference to the modalities of documentation and of filing of the acts of the procedures in order to prevent the transparency and verifiability of the same;
- omitted supervision, control and vigilance on the forms of behaviour of one's own subordinates in order to verify their actions within the scope of the areas at risk of crimes;
- non-observance of the obligation of notifying the Supervisory Body and/or one's line manager about incorrect and/or anomalous and/or irregular forms of behaviour one may have direct and certain evidence of.

The Company may decide on the worker's precautionary suspension with immediate effect.

In case the Company decided to go ahead with the dismissal, the same shall take effect on the day when the precautionary suspension started.

8.7 Administrators and General Manager (Top-ranking positions)

8.7.1 Field of Application

As per art. 6 of the Decree Law 231/2001, the Administrators and the General Manager can be sanctioned in case of:

- non-compliance with the specific protocols (procedures and requirements) provided for by the Model as per DL 231/2001 aimed at programming the training and the application of Company's decisions with reference to crime prevention;
- non-compliance with the rules provided for by the Code of Ethics;
- violation of the provisions with reference to the signatory powers and, in general, to the system of proxies (above all, the requirements related to the modalities of matching);
- violation of the measures related to the management of financial resources;
- violation and/or circumvention of the internal control system provided for by the Model by the means of the destruction or alteration of the documentation provided for by the protocols (procedures and requirements), or by preventing the Subjects in charge of verifications from controlling or accessing the information and the other documentation, there included the Supervisory Body;
- violation of the obligations of informing the Supervisory Body and/or any eventual Subject above the same provided for by the Model;
- upon the exercise of their hierarchic powers and within the limits deriving from the system of proxies, the non-compliance of the obligations of control and vigilance on the forms of behaviour of their subordinate workers. Subordinate workers are only those workers who operate within the scope of the areas at risk of crime and who directly and immediately report to the Senior Manager.

8.7.2 Protection Measures

The Administrator and/or the General Manager who have violated what provided for by the Model and the Code of Ethics, shall be sanctioned based on the gravity of the offence committed:

- written reprimand;

- revocation of the proxies;
- dismissal.

Written reprimand

A written reprimand shall be issued in those cases of violation of the requirements of the Code of Ethics and of the procedures provided for by the Model, except for what provided for in the following paragraph.

Revocation of proxies and/or dismissal

The Administrator and/or the General Manager shall have their proxies revoked and/or shall be dismissed in serious cases of violation. This shall also happen in case of repeated breaches of the requirements of the Code of Ethics and of the procedures provided for by the Model.

8.7.3 Sanctioning Procedures

The Board of Directors is in charge of eventually deciding on the protection measure of the Administrators' revocation of proxies. The Board is also responsible for deciding on the dismissal of the General Manager.

Where the disciplinary measure decided is the one of the dismissal of a Member of the Board of Directors, the Shareholders' Meeting is the body responsible for the decision. The Shareholders' Meeting is summoned by the President of the Board of Directors based on the decision of the same Board of Directors or, if this were not available, by the President of the Board of Statutory Auditors.

For the owners of Functions or of Management, the removal from office will be carried out based on the modalities of the relationship they have with the Company.

Without prejudice to the application of the precaution measure, the Company has the right to propose actions of liability and/or compensation.

Paragraphs 8.3 and 8.4 are applied.

8.7.4 What happens if a Subject holds more than one position

If a Senior Manager also holds a position of subordinate worker and breaches the requirements and provisions in his/her role as Senior Manager, the sanctions provided for by paragraph 8.7.2 shall apply, without prejudice to the applicability of the various disciplinary actions that can be exercised based on the subordinate work relationship existing between the Subject and the Company and in compliance with the legislation procedures - as applicable.

8.8 Auditors

If one or more Statutory Auditors violates this Model and the Code of Ethics, the Supervisory Body shall inform the whole Board of Statutory Auditors and, through the President of the Board of Directors, also the same Board. The latter shall evaluate the notification and then shall activate the Shareholders' Meeting for the adoption of the most appropriate measures.

8.9 External Collaborators

8.9.1 Field of Application

In compliance with the contracts that rule the relationship between the Company and the Collaborators, the external Collaborators subject to vigilance can be sanctioned in case of:

- violation of Company's Code of Ethics;
- fraudulent circumvention of requirements related to the subject of their contract of collaboration having external relevance, or violation of the same by the means of forms of behaviour unequivocally aimed at committing an offence that implies the "Company's Administrative Liability", as per DL 231/2001;
- violation and/or circumvention of the control system put into place by the Company by the means of the theft, destruction, or modification of the documentation related to the conferred assignment;
- missing, incomplete or false documentation of the activities subject of the conferment as to prevent the transparency and verifiability of the same.

8.9.2 Protection Measures

According to what provided for by the specific clauses expressed in the letters of appointment or, more in general, in the contracts, every external collaborator's form of behaviour that integrates the violations as per the previous paragraph and that may imply the risk of the committing of a crime punishable as per. 231/2001 may cause a written warning, the termination of the contract, or any other sanctioning measure (penalties). This shall not affect the Company's right to ask for compensation in case it were to suffer concrete damage.

9. COMMUNICATION AND TRAINING

9.1 Employees' Communication and Training

For the purposes of the efficacy of this Model, the Company aims at guaranteeing a correct knowledge of the rules of conduct present in the Model and in the Code of Ethics, both to the Employees already present in the Company, and to the ones that are to start their working activities with the same. This shall be done with an in-depth analysis related to the different levels of involvement of the same Resources into the sensitive processes.

• Initial communication

The adoption of this Model is communicated by the General Manager to all Employees present in the Company after the adoption of the Model.

All employees are given – by hand or via email or electronic support – a copy of the Code of Ethics, of the Model and of the corporate procedures/rules/recalled regulations (if the latter have not been distributed yet). A copy of the DL 231/2001 is also given to them. Upon receiving these documents, the Workers shall sign a declaration whereby the promise to respect the Model and the Code of Ethics. This declaration is filed and stored by the Supervisory Body.

When a new work relationship is started (of whatever nature it may be), what here-above is to be respected.

Every other piece of information concerning the application of the Model and of the Code of Ethics, (Service Orders, Organisational Communication, Operative Provisions etc.) are distributed to all the people involved and/or hung on the noticeboard.

• Training

The training activities are aimed at spreading the knowledge of the Legislation as per DL. 231/2001 and of the Model and Code of Ethics adopted by the Company. Training shall be managed by the person responsible for the Administration & Personnel Area, in cooperation with the Supervisory Body. Training is differentiated based on the Addressees' different roles. It is also differentiated based on the risk level of the area they work in and whether they carry out Company's representative functions or not.

The training tools identified by the Company are stated here-below:

- initial training course for every newly hired member of staff;
- eventual updating e-mails or meetings;
- eventual in-depth analyses by the means of the attendance to seminars, courses etc.
- Information for the newly hired members of staff in Company's offices.

All training programmes have a common basic content. This consists in the explication of the principles of the DL. 231/01, of the elements that constitute the Organisation, Management and Control Model. The single types of crime provided for and the forms of behaviour considered sensitive with reference to the committing of the afore-mentioned offences are also explained.

In addition to this common part, every training programme shall be organised, where necessary, in order to give its Attendees all adequate tools to allow them to fully comply with what stated by the Decree with reference to the operational scope and the tasks of the Addressees of the same programme.

Attendance to the afore-mentioned training programmes is obligatory.

9.2 Communication to Company's Bodies

The Model is approved by the Administrative Body; thus, it is meant to be known by all Members of Company's Bodies. A copy of the Model shall be transmitted to the Advisors and to those Statutory Auditors that may eventually not be present during the meeting that approved and adopted the Model.

Corporate Bodies' training shall be carried out according to the modalities provided for by the previous paragraph, without prejudice to the modulation of the same based on the specific competences and the positions covered.

9.3 Communication to External Subjects

Consultants, Interns, and various Collaborators, Business and Financial Partners and Suppliers shall be made aware of the Company's adoption of the Model. They shall be asked to comply with the principles described in the Code of Ethics and in the Model (depending on the various cases) adopted by EP. The same shall be made aware that the Company expects that their behaviour complies with what stated by DL. 231. Such commitment is to be provided for by a specific clause in the related contract with acceptance of the contracting Third-Party. Alternatively, with a specific separate declaration, they are to commit themselves to observing the principles of the Model and of the Code of Ethics during the carrying out of their tasks related to sensitive processes and in any other activity that may be executed in the interest and to the advantage of the Company.

SPECIAL PART A): CRIMES AGAINST THE PUBLIC ADMINISTRATION

A.1 Scope of this Special Part

This Special part makes reference to the behaviour of the Company's employees as well as its consultants and collaborators (the "recipients") with reference to the setting up of partnerships with the Public Administration (including the one of foreign countries) and the Authorities.

The objective of this Special Part is that all recipients are to adopt rules of conduct that comply with what here-below stated, in order to prevent the crimes described therein.

In particular, this Special Part aims at:

- describing the protocols and the procedures the Company's employees, its Bodies, consultants and collaborators are to respect in order to correctly apply the Model;
- giving the operative tools to carry out the planned activities of control, monitoring and verification to the Supervisory Body (SB) and to the people responsible of the other company's functions that cooperate with the SB.

Attachment 3 contains a detailed description of the crimes against the Public Administration stated in articles 24 and 25 of the Decree Law 231/2001.

A.2 Areas and Processes at risk and involved Functions

The crimes taken into consideration by this Special Part presuppose the setting up of a partnership with the Public Administration (PA). Thus, all those business areas that deal with the Public Administration for the carrying out of their activities are to be considered at risk. Support or Instrumental areas are those business areas that manage financial tools and/or other means. Even though they are not directly in contact with the Public Administration, these areas can support the committing of crimes.

Bearing in mind the multiple relationships the company has with the Public Administration in Italy, the following activity areas have been identified as being more specifically at risk :

Areas at risk of crime:

Management of relationships with Institutions and Public Bodies, even foreign ones;

Management of disputes, of legal issues and company's business ;

Personnel's Administrative Management ;

Management of the relationship with Supervisory Bodies;

Fiscal Administration, financial statements;

Management of the activities on Public Administration's IT systems;

Data Management of the system

Support/instrumental areas:

Purchasing;

Administrative Management of active contracts ;

Administrative Management of passive contracts;

Budgeting and reporting;

Personnel's selection ;

Management of secretarial activities;

Management of company's communication and of promotional activities.

Sensitive Activities	Area/Function	Possible Crimes
relationships with Public Administration's members who are competent in legislative regulatory or administrative processes, and/or are competent in control processes concerning the Company, when such relationships (there included the sending of data or information) may cause the obtaining of relevant advantages for Public Bodies (Parliament and Senate, Ministry of the Environment, Regions, Councils, Environmental Control Bodies etc.) (however, the activities of mere information, the participation in events or institutional moments and the exchange of opinions with reference to some specific policies or rules and regulations are not considered at risk)	President; General Manager; Responsible for the development of Uses and Regulations District Oversight Function External Consultants	Corruption Instigation to corruption Undue Induction
Activities of lobbying and of technical interlocution with Public Institutions (monitoring of rules and regulations of company's	President; General Manager;	corruption Instigation to

interest in the various phases of approval and at communitarian, national and regional levels; participation in territorial, environmental workshops etc.)	Responsible for the development of Uses and Regulations District Oversight Function External Consultants	corruption Undue Induction
Management of the relationship with public entities for what concerns safety and hygiene on the workplace (Decree Law: 81/2008)	Employers RSPP (Responsible for the Service of Prevention and Protection) Resp. Operations and Logistics	Corruption Instigation to corruption Undue Induction Fraud against the State or any other Public Entity
Management of relationship with Supervisory Bodies related to the carrying out of activities ruled by the Law (Antitrust, Privacy Guarantor, etc.)	President General Manager Responsible of involved dept.	Corruption Instigation to corruption Undue Induction .
Preparation of tax declarations, withholding agents or other statements functional to the payment of taxes in general	External Consultants Responsible for the Administration and Staff	Fraud against the State or any other Public Body
Management of the activities of payment of fees, taxes, INAIL contributions etc.	External Consultants Responsible for the Administration and Staff	Fraud against the State or any other Public Body
the participation in tenders or direct negotiations issued by Italian or Foreign Public Bodies for the awarding of public contracts, concessions, partnerships, research activities, or other similar operations	General Manager Responsible for the development of Uses and Regulations Resp. Operations and Logistics External Consultants	Aggravated fraud for the purpose of obtaining public funds; Fraud against the State or any other Public Body Corruption; Instigation to corruption Undue Induction ;
realization of Projects (Programmes/Activities financed by the means of Public Funds /even European Ones)	General Manager Responsible for the Administration and Staff Responsible for the development of Uses and Regulations	Aggravated fraud for the purpose of obtaining public funds; Fraud against the State or any other Public Body Unlawful obtainment of funds to the detriment of the State; Embezzlement to the detriment of the State
carrying out of procedures for obtaining the authorizations related to the accreditation and the validation of the eco-fees for ELT disposal	President General Manager Responsible for the Administration and Staff	Corruption; Instigation to corruption; Undue Induction Fraud against the State or any other Public Body
Contact with Public Bodies for the management of legal obligations, checks, inspections (PROTECTION AND CONTROL BODIES, MINISTRIES, ARPA, NOE, ISPESL, USL, FIRE BRIGADES, ITALIAN FINANCE POLICE, MUNICIPAL POLICE AND COUNCIL TECHNICIANS, LABOUR INSPECTORATE, INAIL, INPS, PROVINCIAL LABOUR OFFICE)	President General Manager Single Function involved External Consultants	Corruption; Instigation to corruption; Undue Induction Fraud against the State or any other Public Body
management of any eventual litigations and out-of-court disputes	President General Manager Appointed Consultants	Corruption; Instigation to corruption; Undue Induction
activities that provide for the management and control of software of Public Bodies or supplied by third parties on behalf of Public Bodies (SISTRi, Inland Revenue's software, CCIAA, etc.)	IT services District Oversight Area Function Responsible Operations and Logistics	IT fraud; Fraud against the State or any other Public Body
Management of system data (SAP) and of ELT chain data	General Manager Responsible for the Administration and Staff All other functions with reference of their areas of competence	IT fraud; Fraud against the State or any other Public Body
Activities linked to the obligations as per MD 82/2011 (data collection, verification and communication to the Authority of Competence at the Ministry of the Environment)	General Manager Responsible for the Administration and Staff District Oversight Area Function External Consultants	IT fraud; Fraud against the State or any other Public Body
Management of personnel's expense sheets (instrumental)	The involved competent functions	

supply of goods and services (instrumental)	The involved competent functions	
Consultancies and professional services (instrumental)	The involved competent functions	
management of representation expenses, gifts, sponsorships (instrumental)	The involved competent functions	
personnel's hiring with any type of contract (instrumental)	The involved competent functions	
transactions that cause the handling of financial resources (instrumental)	The involved competent functions	
Operations with business partners (instrumental)	The involved competent functions	

Any eventual integration of the afore-mentioned risk areas, there included the ones related to the mapping of the same, may be ordered by EP's President and/or General Manager. They may be given mandate to identify the related hypotheses and to define the appropriate operative measures, without prejudice to the obligation of presenting the news to the first possible Board of Directors.

A.3 General Behavioural Principles – Prohibitions and Obligations

The following general behavioural principles shall apply to the recipients of this Model who, for whatever reason, have a relationship with the Public Administration (there included the people in charge of public service) on behalf of the company or in its interest.

Generally speaking, these people are forbidden from starting, collaborating or give rise to a number of attitudes that, taken individually or collectively, integrate or may integrate, directly or indirectly, the types of crimes provided for by art. 24 and 25 of the Decree Law 231/2001. It is also forbidden to behave in a way that could create a situation of conflict of interest towards the representatives of the Public Administration.

Each Recipient is to carry out his/her relationship with the public Administration following the principles of loyalty, correctness and transparency.

In particular, coherently with the Company's deontological principles expressed in its Code of Ethics, it is **forbidden to:**

- Promise to or make money payments in favour of Italian or foreign Public Administration's Representatives, for aims different from the institutional and service ones and in violation of what provided for by the law.
- distribute gifts and presents exceeding the value stated in the Company's policy (that is: every form of gift exceeding normal business or courtesy practices, or in any case, aimed at obtaining favourable treatment in the carrying out of company's business). In particular, it is forbidden to make any form of gift to Italian and foreign Public Officers or to their relatives (also in those countries where gift-giving is considered normal practice). This is due to the fact that it may influence the independence of judgement or induce to assure any advantage for the company.
- the allowed gifts are characterised by their little value and, in any case, such as not to compromise the integrity or the reputation of one of the parts. They are not to be interpreted as aimed at gaining advantages in an inappropriate way by an impartial observer. In any case, this type of expenditure is to be authorised by the people stated in the specific procedure. Moreover, it has to be adequately documented .
- Promise advantages of any type (e.g.: hiring promises) in favour of Italian or Foreign Public Administration's members of staff or any of their relatives, in order to influence their judgement or induce them to assure any advantage for the Company.
- make unjustified representation expenses and with aims different from the mere promotion of the Company's image.
- carry out services or payments in favour of collaborators, suppliers, consultants, partners or other third party subjects that operate on behalf of the Company, which may not be adequately justified within the scope of the contract entered with the same people.
- In the purchasing process, it is forbidden to favour collaborators, suppliers, consultants or other third parties indicated by representatives of the Italian or foreign Public Administration as a condition for the carrying out of future activities.
- give or promise to release confidential information and/or documents.

The afore-described prohibitions are applicable also to Italian or foreign Public Administration's personnel's indirect relationships (relatives, friends ...).

Moreover, with regards to the Italian or foreign Public Administration, as well as with reference to private people, it is **forbidden to:**

- show documents and false or altered data.
- carry out unnecessary services or invoice for services not effectively provided.
- behave in a way that may lead the Public Administration into a technical-financial evaluation error upon requesting and/or reporting phases related to the awarding of funding or benefits of various nature.
- Omit necessary information in order to influence the Public Authority's decision to Company's advantage.

- Destine contributions, funding, public financing to aims different from the ones they were awarded for
- The Recipients are also **obliged** to respect the following provisions:
- In case of attempted extortion from the part of a public officer, the person involved has to:
 - (i) Not satisfy his/her request;
 - (ii) promptly warn his/her Responsible (in case of Company's employees) or the internal person of reference (in case of third party subjects) and activate the formal communication procedure to warn the Supervisory Body .
 - In case of conflicts of interest arising within the scope of the relationship with the Public Administration, the involved person is to promptly warn his/her Responsible (in case of Company's employees) or the internal person of reference (in case of third party subjects) and activate the formal communication procedure to warn the Supervisory Body.
 - In case of doubts towards the correct application of the behavioural principles here above during the carrying out of their operative activities, the person involved is to promptly warn his/her Responsible (in case of Company's employees) or the internal person of reference (in case of third party subjects) and formally ask for the Supervisory Body's opinion.

The Company is to bestow corresponding powers on those Employees, Company's Bodies, Consultants and Partners who are effectively in contact with the Public Administration on its behalf (with appropriate proxy for the Employees and the Company's Bodies or described in the related consultancy or partnership contract for the other indicated subjects). When necessary, a specific written authorisation will be given to the afore-mentioned people.

The contracts between the Company and Third Parties (Consultants, Partners, Suppliers, Contractors, etc.) are to report in writing all their terms and conditions and respect what stated in the points here-below.

- The contracts with Third parties are to contain standard provisions, commonly defined by the Supervisory Body and the Legal Department in order for them to respect the Decree Law 231/2001.
- The Third Parties are to be chosen with objective and rational criteria as well as respecting a specific procedure (e.g.: by using specific check lists or a formalised procedure). In any case, they are always to be selected in accordance with any eventual criteria set by the Law (by way of example: in case of tenders, criteria for establishing a third party's technical-professional suitability or, where necessary, the fact they belong to certain associations/registers, or their possession of certain professional and technical skills and any eventual certifications)
- In the contracts with Third Parties, a specific declaration of the same is to be included. In this declaration the Third Parties are to state:
 - i) that they are aware of the regulation as per Decree Law 231/2001 and of its implications for the company,
 - ii) that they have never been involved in legal proceedings related to the crimes described in the same (or, if they have been, they are to declare it, so that the Company may pay greater attention upon setting up a contract with them),
 - iii) to commit themselves to behave in a way such as not to commit the crimes provided for by Decree Law 231/2001.
- in the contracts with Third Parties, a specific provision is to be included that rules what consequences they shall suffer for committing (or trying to commit) the crimes as per Decree Law 231/2001 (e.g.: expressed cancellation clauses or penalties).

In the written contracts with business partners the following is to be guaranteed: (i) the definition and presentation of their responsibilities, their operative or control activities etc.; (ii) the definition and sharing of the modalities and procedures the service is to be supplied with; (iii) the introduction of standard provisions to the aims of preventing the crimes as per Decree Law 231/2001 (e.g.: supplier's commitment to describe the controls they put in place to guarantee the respect of the Decree Law 231/2001).

In case of judiciary, tributary and administrative inspections, (e.g.: related to the Decree Law 81/2008, tributary, environmental, INPS and ASL controls, etc.) the specifically delegated subjects are to be present and interact with the Inspection Bodies. In case the Inspection Bodies detected any non-conformities in the final report written by the Company, or critical issues were to arise from the subjects appositely delegated by the Company, the Responsible of the involved Function shall promptly send written warning to the Supervisory Body with the help of the delegated subjects.

The statements sent to national or EU Public Bodies for obtaining financing or contributions made by subjects acting in the name and on behalf of the Company are to contain only truthful elements (in case of prognostic data, they are to be correctly elaborated). In case public funding or contributions were awarded, an appropriate report on the effective use of the obtained funds is to be prepared.

Those who carry out a control and supervision function on obligations linked to the carrying out of the afore-mentioned activities (payment of invoices, destination of funding obtained from the State or EU's bodies, etc.) are to

pay particular attention to the implementation of the same obligations and immediately report any eventual situations of irregularities and anomalies.

A. 4 Internal Control System - Specific Procedures

Within the Company, it is possible to find a specific system of prevention and control for avoiding to commit the crimes described in the Decree Law 231/2001 and related to this Special Part “Crimes against the Public Administration”.

All rules, procedures and tools stated here-below are, in their turn, based on the guiding principles mentioned in the General Part of this document, namely on the requisites of formalisation and clarity, communication and separation of roles, clear attribution of responsibility, definition of the hierarchical rules and the operative activities.

The control system is carried out by all recipients of this Model, each one based on their responsibilities.

Such system is always put into place and is at the base of the fulfilling of all identified sensitive activities. The aforementioned subjects are to respect it. It consists of:

1. **Adoption of the Code of Ethics**, containing specific behavioural principles also with reference to the relationship with the Public Administration (Attachment 2);
2. **Adoption of organisational tools** such as organigrams and organisational communication, aimed at making the company’s internal structure public and to explicitly and formally define the roles (Attachment 1 and at the Company’s offices);
3. **Formal attribution of the power of attorney and expenditure powers to third parties.** This shall be done by the means of a system of specific proxies conferred by the Board of Directors or with notarised power of attorney (at the company’s office and/or published in the competent Company Register);
4. **Attribution of functions and operational responsibilities**– without formal external representation– to the internal resources reflected in the hiring letters, in the system of organisational communications and in *ad hoc* operative and functional proxies (at the Company’s offices);
5. **Estimate and clear highlighting of specific behavioural prohibition and obligations** in this Special Part (paragraph A.3);
6. **Adoption of safety measures on IT systems and data management by the means of the Security Plan Document (DPS) adopted as per Decree Law 196/2003** (at the Company’s offices);
7. **Adoption of specific procedures, rules and company policies** that define roles and responsibilities of the involved functions. They also provide for a series of operative steps and controls to mitigate the risk factors which are characteristics of every area of reference. More in detail, the procedures and the policies are characterised by the following elements:
 - Role segregation;
 - Written track of the relevant process passages;
 - Adequate control .

The procedures, rules and company policies are to be communicated and/or put at disposal of the recipients at every office or involved area. They are described here below. Moreover, they are here reminded because they constitute integrating and substantial part of this Model:

Management of relationship with Institutions and Public Bodies;	Operating practices
Management of judicial disputes	Operating practices
Management of personnel's selection and administration	Personnel's selection Company
Administration and financial statements	Operating practices
Management of purchases	Company's Rule 6
Management sponsorships/ Workshops	budgeting process
Cash Flow Management	Operating practices
Management of gifts and representation expenses/expense reports	Company's rules 4 and 5
Financial flow Management	Use of SAP management system
ELT chain data Management	Use Elties software –on site checks
District Oversight Control Management	The company is implementing Policy
Tender Management	<i>pre</i> and <i>post</i> qualification standards (ref. “Priority Requisites for supply awarding”; typical contractual provisions for bidding companies’ requisites; highly specialising requisites requested to take part to the tenders opened by EP, etc.)

8 Actuation of constant and precise monitoring, making specific reference to incoming and outgoing cash flow, by the means of the adoption of a SAP integrated management IT system. The main characteristic of the SAP software is the one of being able to allow to process data “in real time”. This guarantees essential and transversal functions, such as: system login, menu, customising and enhancement.

Management control as well as all financial and accounting processes, such as: general accounting, the definition and the updating of costs, petty cash book recordings, budgeting, cost centres and cost distribution rules are carried out by the means of the afore-mentioned software. This verifies the correspondence between the purchase order-goods reception and services-payment-invoicing.

For what concerns the management of purchase orders, invoicing and payment systems, there are consolidated company’s policies and regulations. Thanks to the separation of competences and proxies, it is possible to carry out crossed controls between those who make the purchasing request (The responsible of each division), those who authorise and make the payments (General Manager), and those who make the accounting checks (Responsible for Administration and Personnel). In any case, a purchasing management procedure implementation process is ongoing (Company’s rule n 6)

- 9 Making specific reference to the collection of the data related to ELT management, actuation** of constant and precise monitoring and checks by the means of the use of the IT system and of on-site controls of the Area Oversight Function.
- 10 Planning of periodic and constant information flows** towards the Supervisory Body (Paragraph A.5 and General Part).
- 11 Planning of information and training activities** about the Model and the procedures (General Part) as well as about the correct external communication of data and company’s activities ;
- 12 Planning of an adequate sanctioning system** for the breach of rules of the code of Ethics and of the Model, there included the procedures (Disciplinary System – General Part).

A. 5 Information flows

In general, all company’s roles involved in the afore-mentioned activities are to inform the Supervisory Body with reference to situations, news or data they may get to know and that may constitute a breach of this Model and/or the Code of Ethics. They are to do the same with everything that may be of help for a better definition and application of the adopted procedures.

The Responsible(s) identified by the Company has/have the responsibility to prepare a 6-monthly information report for the Supervisory Body about:

- the most significant activities that involved the Public Administration;
- any inspection underwent and the observations eventually formalised by the inspectors, as well as the eventual corrective actions taken;
- judicial procedures started by or against the Company and the results of the same;
- gifts that exceed a certain value;
- the organised sponsorships/workshops the public bodies are involved in;
- the list of people hired in derogation to the principles defined by Company’s procedures;
- the modification of the system of delegations and proxies.

The People responsible shall also promptly inform the Supervisory Body (SB) about all situations that breach –or may breach- this Model and/or the Code of Ethics. They are also to inform the SB about all eventual (motivated) exceptions to the procedures provided for.

A.6 Supervisory Body’s duties

The Supervisory Body periodically carries out random checks on the activities connected with sensitive processes. These checks aim at verifying the correct execution of the same activities with regards to the rules as per this Model. In particular, with the support of the other competent Functions, the Supervisory Body periodically checks:

- the ongoing system of delegations and proxies and their coherence with the whole system of organisational communication;
- the ongoing sensitive operations and storage of their related documentation;
- the sponsorships and donations made;
- the ongoing relevant relationships with third parties.

The Supervisory Board examines any eventual specific alerts coming from control bodies, third parties or any Company’s member of staff. Moreover, it carries out all necessary or appropriate checks as a consequence of the alert.

With regards to the control activities attributed to the Supervisory Board in this Model, the same SB is guaranteed free access to all Company's documentation it may consider relevant for the monitoring of the sensitive processes/activities identified in this Special Part.

SPECIAL PART B): Corporate Crime

B.1 Aim of this Special Part

This Special Part makes reference to the behaviour of Company's Employees and Bodies, as well as its Consultants and Collaborators.

Objective of this Present Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what here-described, in order to prevent the committing of Corporate Crimes.

In particular, this Special Part has the aim of:

- Indicating the protocols and procedures the Company's Bodies, its Employees, Collaborators and Consultants are to respect for the correct application of the Model;
- Giving the operative tools to allow the Supervisory Body and the People Responsible of the other Company's Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities.

Attachment 4 contains the detailed indication of Corporate Crimes recalled by art. 25 ter. of the Decree Law 231/2001.

B.2 Areas and Processes at risk and involved Functions

The main activities at risk the Company has internally identified are the following:

- Preparation of the balance sheet and of the notifications to Business Partners and/or Third Parties about the Company's economic, patrimonial and financial situation (Report on Management, Notes to the Financial Statement, etc.);
- Operations related to share capital, mergers, demergers;
- Management of relationships with Supervisory Bodies (Auditing Firms, Board of Auditors, etc.)
- Eventual drafting of notifications to Public Supervisory Bodies and management of relationships with the same Public Supervisory Bodies (the Italian Competition Authority, "Antitrust", Data Protection Authority, etc.).
- Preparation and external divulgation of information prospects and/or data or news related to the Company and the Companies of the Consortium;
- Management of relationships with Consortium Companies;
- Management of relationships with Suppliers.

In the following table the sensitive activities are reported. Also the Areas/Functions at risk of committing crimes and the possible crimes are reported.

For what concerns the identification of the involved corporate Functions, it is necessary to bear in mind that the majority of corporate Crimes fall within the category of the so-called "proper" crimes. With reference to this type of crimes, in theory they can be committed only by those who hold the subjective professional qualification stated by the legislator (for example: administrators, liquidators etc.).

Such circumstance does not exclude, however, the possibility that also the other corporate Functions may be involved in the committing of the crime, as per art 110 of the Penal Code. Thus, every Company's resource may in theory contribute in the committing of the crime.

Sensitive Activities	Area/Function	Possible Crimes
Exposition and gathering of useful data for the drafting of the financial statements	General Manager, Administration and Personnel Area	False corporate communication
Writing of the financial statements project and periodic reports	President, BoD, General Manager, Board of Statutory Auditors, Administration and Personnel Area, External Fiscal Consultant	False corporate communication
Financial statement approval	President and BoD, Assembly of Statutory Auditors	False corporate communication
Writing of prospects of various nature	General Manager, All other involved functions	False corporate communication
Operations on the capital	President, BoD, General Manager and Consultants (preparation of Acts)	Undue contributions refunds, Illegal allocation of profits/reserves, operations to the damage of creditors, Fictitious formation of capital
Relationship with Partners, Board of Statutory Auditors, Firm of Auditors	President, BoD, Statutory Auditors, External fiscal/judicial consultant Involved Functions	Prevented control, False corporate communication, Corruption among private people

Relationship with Control Bodies	President, BoD, General Manager, Administration, Statutory Auditors, External Consultants and involved Functions	Obstruction to the exercise of the functions of the Public Supervisory Authorities
Issue of press releases	President, General Manager, External Consultants	False corporate communication
Communication, carrying out and recording of Partners' Meetings	President, BoD, Statutory Auditors Person Responsible for Admin and Personnel	Illicit influence on the Assembly, False corporate communication
Communication, carrying out and recording of Board of Directors' Meetings	President, BoD, Statutory Auditors, General Manager, Person Responsible for Admin and Personnel	False Company Communication
Relationships with Consortium Companies	BoD, General Manager, Responsible for Admin and Personnel	Corruption among private people, Instigation to corruption among private people
Relationships with suppliers and Third Parties in general	General Manager Responsible for Admin and Personnel	Corruption among private people, Instigation to corruption among private people

B.3 General principles of behaviour – Prohibitions and Obligations

It is forbidden to put in place, collaborate with, or cause forms of behaviour that, taken individually or collectively, may directly or indirectly integrate the types of crime described by art 25 ter. of the Decree Law 231/2001. The violations of the Code of Ethics and Company's procedures are also forbidden.

In order to avoid Corporate Crimes, all Recipients **are obliged to:**

- Keep a conduct based on the principles of correctness, transparency, and collaboration in the carrying out of the procedures aimed at the drafting of the financial statements, the periodic accounting statements and corporate communication in general;
- Keep a form of conduct based on the principles of correctness, transparency and collaboration upon obtaining, elaborating and communicating information to allow the interested Third Parties to form their opinions and/or judgement on the Company's patrimonial, economic and financial situation;
- Give true and appropriate information on the Company's patrimonial, economic and financial situation;
- Assure the smooth running of the Company and its Bodies, facilitating and guaranteeing every form of internal control and promoting free information and the taking of collegial decisions;
- Scrupulously respect all Laws protecting the integrity and effectivity of share capital;
- Collaborate in the achieving of Company's business objectives;
- Observe the Laws on the protection of market competition and make sure that the same Laws are perfectly respected. Moreover, they are to collaborate with the market Regulatory Authorities and with the other Supervisory Bodies.

Moreover, it is forbidden:

- to prepare or communicate false or incomplete information or, in any case, any type of data that may represent reality in a distorted way with reference to the economic, patrimonial and financial situation of the Company and its Partner Companies, as well as the evolution of all related activities;
- in particular, to input false or incomplete data in the SAP IT system;
- to omit to communicate data or information required for by the Law and by the Procedures in force, with reference to the economic, patrimonial and financial situation of the Company and/or its Partner Companies;
- to alter or, in any case, to report data and information destined to the drafting of information prospects in an incorrect way;
- to return contributions to the Partners or to exempt Partners from making them, to the exception of those cases specifically provided for by the Law;
- to carry out profit sharing operations that cannot be made by Law or by Articles of Association;
- to buy shares of the Company outside of those cases provided for by the Law or by the Articles of Association;
- To carry out reductions of share capital, mergers or demergers in violation of what stated by the Law for the protection of creditors;
- To go ahead with the formation or the fictitious increase of share capital in any way;
- Upon liquidation, to share corporate goods among Partners before corporate creditors have been paid or the provisions of the necessary money to comply with them have been made;

- To behave in a way that materially prevents (or may obstacle in any case) the carrying out of the activities of control or revision of Corporate Management from the part of the Board of Statutory Auditors by the means of the hiding of documents or the use of other fraudulent means;
- On the occasion of meetings, to put in place simulated or fraudulent acts, aimed at altering the regular process of expression of the will of the participants to the meeting;
- To put in place any form of behaviour that may obstruct the activities of the Public Supervisory Authorities even upon inspection phase (expressed opposition, pretentious refusal, outright obstructive behaviour or lack of collaboration, such as: delays in notifying the Authorities or in providing them documents);
- To omit to notify the Supervisory Bodies with the appropriate quality and promptness as per what stated by the Law. To omit to send data and documents provided for by the Legislation and/or required by the aforementioned Authorities.
- To promise to make (or effectively make) money payments in favour of Third-Party Subjects for aims different from institutional and service ones and in violation of the legislation.
- To promise or give advantages of all types (e.g.: hiring promises) in favour of Third-Party Subjects or their relatives, in order to obtain forms of behaviour that may damage the Company they belong to and gain an illicit advantage for Ecopneus

B.4 Internal Control System – Specific Procedures

The Control System for the prevention of those crimes stated in the DL 231/2001 and related to this Special Part, “Corporate Crime”, is composed of the following elements. In their turn, these are based on the principles mentioned in the General Part of this document, namely, on the requisites of formalization and clarity, communication and separation of roles, clear attribution of responsibility, definition of hierarchies and operating activities.

The Control System is implemented by all Recipients, each of them according to their responsibility.

Such System is always implemented. It is also at the basis of the carrying out of all identified sensitive activities the afore-mentioned Subjects are to respect. This System is composed of:

1. **Adoption of the Code of Ethics**, containing specific types of behaviour, also with reference to the principles of accounting and management transparency, correctness in the relationship with Authorities, Partners etc. (Attachment 2);
2. **Adoption of the Code of Self-Discipline of the Administrators;**
3. **Provision and clear highlighting of certain behavioural Prohibitions and Obligations** in this Special Part (Paragraph B.3);
4. **Actuation of a specific and constant monitoring with reference to the entry and management of accounting and financial data.** This is done by the means of the adoption of the “SAP” integrated management IT system. By allowing to process data in “real time”, this system allows a high level of control on the accounting process and data gathering by the means of **traceability of the processes activated through IT systems** (e.g.: recording of events such as accounting adjustments);
5. **Storage and filing** (also electronically) **of all documentation of competence produced** from the part of each Function, in order to allow the reconstruction of the responsibility and the choices made;
6. **Provision of periodic and constant information flows** towards the Supervisory Body (Paragraph B.5 and General Part).
7. **Provision of information and training activities** on the Model and Procedures (General Part)
8. **Provision of an adequate sanctioning system** for the violation of the rules of the Code of Ethics and of the Model, there included the Procedures (Disciplinary System – General Part).
9. **Actuation of constant and precise monitoring with specific reference to the incoming and outgoing money flows.** This is done by the means of the adoption of the “SAP” integrated management IT system.
10. **Adoption of specific procedures, rules and Company’s practices** that define the roles and responsibilities of the involved functions. Moreover, they provide for a number of operative steps and controls to mitigate risk factors that are typical of each Area of reference. More in particular, the procedures and the practices are characterised by the following elements:
 - **Role segregation;**
 - **Written track of the process relevant passages;**
 - **Adequate control**

a) Financial Statements and other forms of Company’s Communication

The Project of the Financial Statements is prepared by the General Manager, checked by the President and finally approved by the Board of Directors. EP avails itself of an external financial Consultant.

The drafting of the annual financial statements and of all communication provided for by the Law sent to Partners and Creditors is to be carried out in compliance with the existing procedures, what stated by the Rules of the Civil Code, and the Accounting Principles based on the following operative procedures:

- Through their managers, the competent Functions identify the data and information to supply for the drafting of the financial statements. To this aim, the following is to be determined in a clear and precise way:
 - the data and information subject of the communication;
 - the data elaboration criteria;
 - the timing for data delivery.
- The data are transmitted to the competent Function (General Manager, Administration and Personnel Area and External Consultant) through the IT system. This allows the tracking of every single passage and the identification of the Subjects that enter the data into the system;
- The prompt transmission of the financial statement draft and of the report of the Board of Statutory Auditors to all members of the Board of Directors, as well as the appropriate recording of such document transmission. In their turn, these are to be handed in to the Supervisory Body;
- Adequate justification, documentation, and related filing of any modification made to the financial statement draft/interim situations from the part of the Board of Directors.

b) Protection of Share Capital

The operations on the Company's share capital, those for the creation of Companies, buying or selling of equities, as well as all those operations that may potentially damage the Company's share capital are to be carried out in compliance with the Rules of the Civil Code and of the Protocols described here-below.

Thus, the following is necessary:

- The awarding of decisional and operative responsibility for the afore-mentioned operations, as well as the coordination mechanisms among the various corporate Functions involved;
- The respect of the General Manager's obligatory opinion, the eventual evaluation from the part of the external Judicial/Fiscal Consultant, as well as the forwarding to the Board of Directors for the approval of corporate operations on Company's share capital (such as: the creation of Companies, the purchasing and selling of equities, the reduction or increase of share capital even by the means of contributions in kind, etc.);
- The information report about each relevant initiative to the Supervisory Body.

c) Ruling Company's operations

In order to prevent the committing of the crime of obstruction of checks on Corporate Management from the part of Corporate Bodies, the following rules have been set.

In particular:

- It is forbidden to materially obstruct the carrying out of control activities from the part of the Board of Statutory Auditors and the Auditing Company by the means of the hiding of documents or the use of other fraudulent means that may, in any case, obstruct what afore-said;
- the General Manager and the Person responsible for the Administration and Personnel Area take care of the relationship with the Control Bodies. Their tasks are of coordinating and collecting information and the documents required by the Control Bodies. They shall also evaluate the appropriateness, completeness and correctness of the documents;
- all documents related to the topics on the agenda of the Board of Directors' meeting are to be promptly transmitted. The same is to be said for those documents the Statutory Auditors are to express their opinion on as per legal requirements;
- the Board of Auditors periodically checks the documents on Company's management;
- during the course of the year, the Auditing Firm checks the correctness of corporate bookkeeping and the correctness of management issues recording in the accounting entries;
- it is possible for the Board of Auditors and the Supervisory Body to call for periodical meetings to verify Management's and Employees' observance of protocols and discipline with reference to Company's rules and regulations.

d) Activities subject to vigilance

In order to prevent the committing of the crime of false notification to the Authorities and the crime of obstruction to Supervisory Functions, the activities subject to vigilance based on specific sector rules and regulations are to be carried out in compliance with the existing corporate procedures. They are also to be executed in compliance with any

other further rule and regulation that may be necessary to implement, as well as the principles of correctness and transparency.

In particular:

- The truthfulness and promptness of documents, data and information given to the Supervisory Authorities is assured in compliance with the principles of collaboration and transparency, also during the course of any eventual inspection;
- The person responsible for the Administration and Personnel Area is in charge of the activities of collection, communication and transmission of such data. This person takes care of the regular execution of every task and of the documentation related to the ongoing activities. This is to be kept at the disposal of the Supervisory Body for eventual checks. Moreover, the afore-mentioned responsible person is to write an annual report on any eventual relationship with the Supervisory Authority;
- The requests for data, all notifications and inspections are to be communicated to the Supervisory Body.

B.5 Information Flows

The General Manager is to transmit a report on the eventual extraordinary corporate operations to the Supervisory Body (mergers, demergers). This report shall also include the constitution of companies, the purchasing and selling of equities, the reduction and increase of share capital, the eventual modifications made to the financial statement project upon request of the Administrative Body and/or the President.

B.6 Tasks of the Supervisory Body

In addition to the tasks described in the General Part and to the specific ones stated in each Special Part, the Supervisory Body is also competent for what here-below described. This guarantees the efficacy of the Model with reference to corporate crime:

- 1) Financial statement and other corporate communication:
 - Monitoring of the efficacy of protocols and procedures for the prevention of the crimes of false corporate communication;
 - Examination of eventual specific notifications coming from Control Bodies or from any Employee and preparation of all checks deemed necessary or appropriate as a consequence of the received notifications.
- 2) Protection of share capital, regular running of the Company and activities subject to supervision:
 - Periodical checks on the respect of protocols and internal procedures;
 - Periodical checks of communication to Supervisory Bodies and of the result or development of eventual inspections;
 - Examination of eventual specific notifications coming from Supervisory Bodies or Employees and preparation of eventual checks.

SPECIAL PART C): MANSLAUGHTER AND SERIOUS OR VERY SERIOUS INJURIES WITH VIOLATION OF THE RULES FOR THE PROTECTION OF WORKERS' HEALTH AND SAFETY

Foreword

The Law n. 123 of 3rd August 2007 was published on the Official Gazette n. 185 of 10th August 2007 and introduced art. 25 septies of Decree Law 231/2001. With this Law, the Legislator provided for the extension of company Bodies' administrative responsibility for the crimes of manslaughter and personal serious injuries committed in violation of the health and safety rules for the protection of hygiene and health on the workplace.

Decree Law n. 81/2008 collected and assembled a number of rules, such as Decree Law 626/1994 (now repealed), thus defining a general system of prevention and safety. The Consolidated Text here-above has summarised the majority of the existing rules and regulations regarding the prevention of professional risks. It has provided for the elimination of risks of accidents, the proposition of the workers' active role and their right to be informed and consulted.

Thus, the principles of this Model are necessarily to be integrated with the provisions already internally applied by the Company in compliance with the Rules and Regulations about health and safety on the workplace. Thus, all documents, rules, provisions and procedures elaborated by the Company in compliance with the legislation in force are here recalled, in particular Decree Law 81/08 and its following modifications and additions.

C.1 Aim of the Special Part

This Special Part makes reference to forms of behaviour of Company's Employees and Bodies, as well as its Consultants and Collaborators, wherever applicable.

Objective of this Special Part is that all afore-mentioned Recipients adopt rules of conduct in compliance with what stated in this Special Part and in all the applicable rules and regulations provided for the prevention of workers' integrity and health. This is to avoid crimes of manslaughter and serious and very serious injuries (as a consequence of the violation of the rules for the protection of workers' health and safety).

In particular, this Special Part aims at:

- Stating the protocols and procedures that the Company's Bodies, Employees, Consultants and Collaborators are to respect for the correct application of the Model;
- Giving the operative tools to carry out all planned activities of control, monitoring and verification to the Supervisory Body and to the People Responsible for other Company's Functions collaborating with the same SB.

Attachment 5 contains a detailed list of the Crimes of manslaughter and serious or very serious injuries from art. 25-septies Decree Law 231/2001.

C.2 Areas and Processes at risk and involved Functions

C.2.1 EP's Organisation with reference to Hygiene and Safety on the Workplace

The General Manager is the Subject who has taken on the role of Employer by virtue of a specific delegation from the Board of Directors. He/she also has managerial powers with reference to financial resources to be destined to crime prevention.

Moreover, the following Functions are present:

- RSPP – Responsible for the Service of Protection and Prevention – external, expressly nominated by the Employer;
- RLS – Workers' Representative for Safety;
- MC – External Competent Medical Doctor, expressly nominated by the Employer.

In collaboration with the RSPP, the Employer deals with the drafting of protocols, procedures, emergency plans management and training also by the means of specialised external consultants. Moreover, he/she also keeps and updates the documents on safety and carries out all suitability verifications of the workplaces in collaboration with the MC (at least once a year).

C.2.2 Areas at risk and sensitive activities

The main risks for committing the crimes here-above described are potentially referable to those people who are responsible for the final decisions about safety expenditure and intervention, namely, the Company's top management and the General Manager.

However, it is here pointed out that, with reference to the mapping of Company's environment, it is not possible to exclude any business domain *a priori* – nor the involvement of other Functions. This is due to the fact that such crimes may involve the totality of the Company's domains, for example: with reference to the choice of the contracting enterprises [see: sentence 26/10/2009 Courts of Justice of Trani, Detached Section of Molfetta].

In order to preliminarily define sensitive activities as per art. 25, septies of the Decree Law. 231/2001, thus, it is necessary to consider the activities where accidents may occur and the ones where a crime may occur due to Company's

negligent infringement of the rules and of the existing preventive measures protecting health, hygiene and safety of the workplace.

To this aim, the crime (serious or very serious injury or death) may be committed by the means of active or negligent behaviour (i.e.: the agent does not intervene to prevent the crime). Usually, an active form of behaviour is the one of an employee who carries out operative tasks directly and who materially damages other people. On the contrary, negligent conduct can be equally identified in the senior management who do not carry out their obligations of vigilance and control and, in this way, they do not intervene to prevent the event caused by others.

The crimes subject of this Special Part may be committed in theory in all those cases in which there is a violation of the obligations and of the provisions with reference to health and safety on the workplace within the Company.

Even in compliance with the existing rules and regulations (DL 81/2008), EP has carried out the evaluation of work risks by the means of the preparation of its own "Risk Evaluation Document" (here below also "DVR").

Sensitive Activities	Area/Function	Possible Crimes
Management of requirements with reference to hygiene and safety on the workplace, as per DL. N. 81/2008 and its following modifications	Employer; RSPP; eventual people responsible/technicians; MC	Manslaughter serious/very serious injuries
Correct and regular application of procedures and legal requirements with reference to hygiene and safety on the workplace, as per DL. N. 81/2008 and its following modifications	All Company's Functions	Manslaughter serious/very serious injuries
Management of Health and Safety with special reference to Human Resources' Training and Information;	Employer; RSPP; Person Responsible for Administration and Personnel; External Consultants	Manslaughter serious/very serious injuries
Management of Health and Safety upon selecting Suppliers/Contractors aimed at the correct execution of the contracts entered with the companies for the correct management of the consortium's activities	General manager; Resp. Operations and Logistics; District Oversight Function; External Consultants;	Manslaughter serious/very serious injuries

C.3 General Behavioural Principles– Obligations and Prohibitions

The Employer, the RSPP, the Delegates and the Employees are to respect the following general principles:

- Guarantee the strict respect of all Laws and regulations in force that rule Company's activities with reference to safety;
- Directly notify the Supervisory Body about all anomalies they have encountered during the monitoring/execution of the obligations with reference to Hygiene and Safety on the Workplace as per DL. n. 81/2008.

Moreover, by the means of the competent Functions (Employer, RSPP, other Delegated Subjects), the Company is to respect what follows:

- Predisposition of Safety procedures, applying what stated in the legislation of the sector;
- Predisposition and/or constant update of the Risk Evaluation Document and/or of similar documents;
- Check of legislative updates with reference to Safety and Hygiene on the Workplace;
- Identification of Prevention and Protection System (SPP) Personnel, also in case emergency situations were to arise;
- Monitoring the effective actuation of the control system described in the Risk Evaluation Document. This provides also for the definition of appropriate corrective and preventive measures wherever non-conformity situations have been identified;
- Verification of constant workers' training with reference to safety and health, bearing particular attention to their workplace and their tasks;
- Verify that a meeting with the Employer, the Person Responsible for SSP, the MC and the Workers' Representative for Safety is held at least once a year;
- Verify that the People Responsible and the People in charge of SSP, the MC and the Workers' Representative for Safety possess all professional requisites and certifications required by the legislation in force;
- Verify that the People Responsible and the People in charge of SSP, the MC and the Workers' Representative for Safety and Hygiene on the workplace attend the effective professional update activities at least every five years;
- in case of whole or partial outsourcing of activities related to the respect of the legislation for Safety and/or protection of Safety and Hygiene on the Workplace, the existence of specific procedures and their related controls is to be monitored within the outsourcing companies.

C.4 Internal Control System – Specific Procedures

Within the Company's Organization, thus, there is a system of prevention and control whose afore-mentioned Subjects are to respect. This system:

- provides for a number of Functions that assure the technical skills and the necessary powers for the verification, evaluation, management and control of the risks identified within the Company;
- assures an adequate recording system of the effective application of what stated by the legislation in force with reference to safety;
- provides for an appropriate control system on the application of the adopted safety measures and on the persistence of the conditions of appropriateness of the same during the course of time;
- is to be reassessed and, eventually, modified whenever important violations of the rules related to accident prevention and hygiene on the workplace were to be identified. The same is to be done in case of changings within the organization and the activities related to Scientific and Technological Progress.

In particular, it is here highlighted:

1. Adoption of the Code of Ethics, containing specific behavioural principles also with reference to Safety and Hygiene of workplaces (Attachment 2);

2. Prevision and clear highlighting of specific behavioural prohibitions and obligations in this Special Part (paragraph C.3);

3. Prevision of Employer's specific proxies and powers within the scope of the sensitive activities of Management of the requirements for complying with hygiene and safety on the workplace as per DL n. 81/2008 and its following modifications, even with explicit reference to the management of financial resources aimed at preventing the committing of crimes (Board of Director's Reports).

4 Written nominations of RSPP and RLS (kept and filed with Company's records);

5. Preparation and constant update of the Risk Evaluation Document (DVR) (kept at Company's headquarters), which is here expressly recalled as integrating part of the Model;

6. Prevision of periodic and constant information flows towards the Supervisory Body (Paragraph C.5 and General Part) that help the vigilance on the application of the Model;

7. Prevision of information and training activities on the obligations laid down by DL 81/2008 – useful also to the aims of this Model – as well as this General Part

8. Prevision of an adequate sanctioning system for the violation of the rules of the Code of Ethics and of the Model (there included also the Special Part), Procedures (Disciplinary System–General Part).

9. Adoption of operative protocols and specific procedures, some of which are currently being implemented. They are here recalled to be integrating and substantial part of this Special Part.

10. In particular, for what concerns preventive measures with reference to safety within the scope of ELT management chain contractors (operators for transport, collection, shredding and valorisation), the Company has adopted an integrated selection and verification system based on:

a) preventive control: the choice of the contractor is always made by the means of a tender with high qualitative standards. These qualitative standards guarantee reliability especially with reference to the issue of Safety on the workplace;

b) control during the carrying out of activities: adoption of a specific programme for the control of the chain technical partners through constant monitoring and verification activities carried out by both the Functions of District Oversight and External Companies of technical auditing (safety and environment).

c) evaluation at the end of the activity: prevision of systems of contractor's evaluation that bear in mind the indexes or scores given to the same contractor by the District Oversight Area Functions following verifications *in situ*. This is done in order to evaluate the reliability of the same contractor.

The Company expects that:

- the controls carried out by the District Oversight Area Functions and by the Company of technical auditing (chosen by the means of a tender) are constant. They are also aimed at ascertaining that the requisites stated by the law on Safety on the workplace are met;
- the results of the afore-mentioned controls are reported in a specific file present on the Company's IT network. Its Type-tab is here attached. From the same, it is possible to see the detailed verifications and controls. This allows the General Manager and the other interested Functions to have a clear and updated pictured of the monitoring activities at any time;
- the tender contracts choose the contractor based on high qualitative standards and precise and rigorous criteria. These tender contracts have to: i) be defined in writing, in all their terms and conditions; ii) contain standard clauses in order to comply with Decree Law 231/01; iii) contain an appropriate declaration of the same in which they state that the contractors are aware of the rules and regulations as per Decree Law 231/01 and that they promise to behave as per what stated in the same law; iv) contain a specific clause that rules the consequences of their violation of the rules as per Decree Law. 231/01 (e.g.: expressed termination clauses,

sanctions).

C.5 Information Flows

In general, all Company's Roles involved in the management and application of what stated in Decree Law 81/2008 are to inform the Supervisory Body about situations, news, or data they may come across during the execution of their duties that may constitute a violation of this Model and/or of the Code of Ethics, with reference to this Special Part. They are to report also situations, news, or data that may be of help for a better definition and application of the adopted procedures.

In agreement with the RLS and the MC, the RSPP has the responsibility of preparing an annual informative report for the Supervisory Body. This report concerns all relevant safety aspects with reference to the potential committing of crimes of manslaughter and serious or very serious injuries as a consequence of the violation of the rules and regulations aimed at protecting workers and the environment they work in.

The President of the Board of Directors or his/her delegate has the responsibility to notify the SB about the modifications to the system of proxies and delegations within the scope of compliance with Safety rules and regulations.

The Person Responsible for Administration and Personnel has the responsibility of transmitting what follows to the Supervisory Body on a six-month basis:

- the list of accidents as reported in the Injury Register (or directly a copy of such Register) that implied an absence from the workplace equal to or higher than 40 days;
- the starting of any eventual procedures for professional diseases/injuries.

Moreover, based on what their competence is and/or in agreement among them, the afore-mentioned People are to provide the SB with what stated here-below:

- a copy of the report of the periodic meeting as per art. 35 DL. 81/2008;
- the results (or copy of the reports) of any eventual audit on safety;
- the results of the checks and of the monitoring activities carried out by the Functions District Oversight;
- Integrations/revisions of DVR;
- The new nominations of RSPP, RLS, MC, people in charge, etc.;
- The eventual inspections of the P.A.;
- The conventions/contracts/etc. whence EP's Employer derives his/her responsibility with reference to Safety (such as, by way of example: where mobile workers are located, tender contracts with the preparation of the DUVRI – the Single Document for the Evaluation of Interference Risks – etc.).

C.6 Supervisory Body's tasks

Without prejudice to the discretionary power of the Supervisory Body of effectuating specific controls following received notifications, the Supervisory Board carries out periodical sample controls on the activities connected to the sensitive processes potentially at risk of crimes of manslaughter and unintentional injuries committed in violation of safety regulations. These controls are aimed at verifying the correct application of the same rules with reference to the principles stated in this Special Part and in the existing internal procedures.

To carry out such periodic controls, the Supervisory Body avails itself of the collaboration of other Company's Functions or of External Consultants.

It is here repeated that the Supervisory Body has the right of free access to all relevant Company's documentation.

SPECIAL PART D): IT CRIMES AND ILLICIT DATA MANAGEMENT

D.1. Aim of this Special Part

This Special Part makes reference to forms of behaviour of Company's Employees and Bodies, as well as its Consultants and Collaborators.

Objective of this Special Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what here-described, in order to prevent the committing of IT crimes and illicit data management.

In particular, this Special Part has the objective of:

Detailing the protocols and procedures the Company's Employees, Bodies, Consultants and Collaborators are to respect, to the aims of the correct application of the Model;

Supplying the operative tools to allow the Supervisory Body and the People Responsible for the other Company's Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities.

Attachment 6 contains detailed indications about IT crimes and illicit data management as per art. 24 bis of the Decree Law 231/2001.

D.2. Areas/Processes at risk and involved Functions

With reference to the crimes described in Attachment 6 and presented in art. 24 bis of the DL. 231/2001, the sensitive activities which are considered mainly at risk are the ones where IT tools are used by the means of an internet connection.

Sensitive Activities/Processes	Area/Function	Possible Crimes
Management of corporate IT systems (installation, maintenance, programming and hardware/software networking, services of hosting/ data management), even by the means of external technicians of outsourcing companies;	Person responsible of IT services, External Consultants (Software house, technical assistance etc.) Administrators and General Manager (Principals/Tenders)	Illegal access to IT systems Illegal detention and spreading of access codes to IT systems Spreading of IT equipment, devices or software aimed at damaging or interrupting an IT system Illicit interception or interruption of IT communication Installation of equipment aimed at intercepting, preventing of interrupting IT communication Damaging of information, data and IT programmes Damaging of information, data and IT programmes used by the State or any other Public Body or, in any case, of public utility Damaging of IT systems IT documentation
Email correspondence with clients, suppliers, offices and Public Authorities (for example: CCIAA, Agenzia delle Entrate, INAIL, etc.), Bodies or competitors	Administrators, General Manager, Person Responsible of Administration and Personnel, External Consultants (Fiscal consultant etc.); Person Responsible for the Development of Use and Regulations, Person Responsible for IT services	IT documentation Illegal access to an IT system Illegal detention and spreading of access codes to IT systems Spreading of IT equipment, devices or software aimed at damaging or interrupting an IT system Damaging of information, data and IT programmes Damaging of information, data and IT programmes used by the State or any other Public Body or, in any case, of public utility Damaging of IT systems IT fraud of the Subject that provides for electronic signature certification services
Relationship with Subjects who supply electronic signature certification services	President, BoD, General Manager, Person Responsible for Administration and Personnel, External Consultants	IT fraud of the Subject that provides for electronic signature certification services IT documentation
home banking activities	President, BoD, General Manager, Person Responsible for Administration and Personnel	IT documentation
use/management of SAP and Elies software for data management;	All involved Functions and interested Subjects	IT documentation

Access to/use of external IT systems

Special attention and diligence shall be paid by Top Management (President, Administrators) and by Senior Management with directive functions (General Manager) in the use of IT systems even outside of the Company Headquarters. This is because the prevention system provided for by this Model is to be considered valid (comprehensive of prohibitions and obligations) for what committed by those same Subjects even by the means of external IT systems and, in any case, connected to the network.

D.3. General principles of behaviour – Prohibitions and obligations

The following behavioural principles of general nature are applied to the Recipients of this Model who, for whatever reason, are involved in Company's "sensitive" activities with reference to IT crimes and illicit data management, either directly or indirectly. In particular, these principles apply to all those people who use IT tools for the carrying out of their working activities in favour of the Company.

In general, such Subjects **are requested to:**

- Scrupulously respect all Rules and Regulations set out by the Law and the internal Company's procedures and Regulations with reference to Company's IT system safety and the management of any data.
- Refrain from putting in place, collaborate or give rise to forms of behaviour that, taken individually or collectively, may integrate the types of IT crimes and illicit data management, directly or indirectly.

Moreover, all afore-mentioned Functions are expressly **obliged to:**

- Promise not to divulge all information at their disposal for the use of IT resources and the access to data and systems (paying particular attention to username and password, which are necessary for accessing the Company's systems).
- Activate every measure deemed necessary for the protection of the system, avoiding that third parties may have access to the same, in case they were to move away from their workstation (exiting the system or access blocking by the means of passwords).
- Access the IT systems exclusively through identification codes assigned to the single Subject and providing for the periodic modification of the passwords, within the deadlines set by the person responsible for IT services, (when provided for).
- Use and correctly keep the Company's digital signatures;
- Keep and file the documentation of competence electronically produced in order to be able to reconstruct the responsibility and the choices made;
- Refrain from putting into practice any form of behaviour that may put at risk the confidentiality and/or integrity of Company's data.
- Not to start actions aimed at going beyond the protections applied to Company's IT systems.
- Not to install any programme, even if linked to Company's activities, without discussing the issue with the Person responsible of the IT systems
- Use exclusively the connections put at their disposal by the Company for the carrying out of their working activities in the Company's offices
- Not to access Third Parties' IT systems in an unauthorised way; not to alter their functioning in any way in order to obtain and/or modify data, programmes or information without having the right to do so.

In case of doubts about the correct application of the ethical-behavioural principles as per here-above during the course of the operative activities, the interested Subject has to make reference to the Person Responsible for the IT services.

Moreover, in order to protect its own IT systems and avoid, as much as possible, its own involvement into activities that may lead to the committing of one or more IT crimes or illicit data management, **the Company commits to:**

- Provide for the possibility of accessing IT systems only following appropriate identification from the part of the User by the means of username and password originally given to them by the Company;
- Establish the modalities of changing of the password after the first access, strongly advising to avoid the use of cyclically repeated passwords;
- Establish the frequency of modification of the same password, according to the use frequency and the criticality of the data accessed by the means of that password;
- Constantly verify the coincidence between the powers assigned to the user profile and his/her tasks within the Company, both in the cases in which a Subject is entrusted with different activities and upon conclusion of the work relationship with the company;
- Periodically monitor all accesses and activities carried out on corporate network;
- Adequately train every Resource on how to behave to guarantee the safety of IT systems and the possible

consequences deriving from the committing of a crime.

Finally, with regards to Third-Party Contractors (e.g.: Collaborators, Consultants, Partners, Suppliers, etc.) involved in the carrying out of activities at risk of IT crimes and illicit data management and who act on behalf of the Company and in its interests, according to specific selection criteria, their contracts are to:

- Be defined in writing, in all of their terms and conditions;
- Contain standard clauses to comply with Decree Law 231/2001;
- Contain an appropriate declaration of the same Subjects. In this declaration they are to state that they are aware of what stated by DL 231/2001 and that they commit themselves to behave in agreement with what stated by the Rules and Regulations;
- Contain an appropriate clause that rules the consequences of their violation of the Rules and Regulation as per DL. 231/2001 (e.g. express termination clauses, penalties).

D. 4. Internal Control System – Specific Procedures

Within the Company, it is possible to find a specific prevention and control system with reference to the prevention of the committing of the crimes described in DL. 231/2001 and making reference to this Special Part, “IT crimes and illicit data management”, the afore-mentioned Subjects are to respect.

1. **Adoption of the Code of Ethics**, containing specific behavioural principles also with reference to the use of IT systems;
2. **Adoption of the DPS (Security Plan Document)** written and adopted by the Company as per DL 196/2003 (Privacy Code). In this document, it is possible to find the detailed security measures of the IT systems, as well as specific protocols of internal prevention and control, in order to avoid intrusions or inappropriate use of the IT systems.

The Code about personal information protection provides for the adoption of security measures aimed at maximally reducing the risks of their (even accidental) destruction or loss. These security measures also maximally reduce the risks of non-authorized data access; they also mitigate the risks of non-allowed data management as well as the ones of data management that do not comply with the aims of data collection. Thus, the Model adopts such recommendations with reference to data protection and to the information managed by the means of IT modalities. It formalises the general principle that all operations, transactions and actions are to be verifiable, documented, coherent and congruous. This principle also states that data protection and IT procedures are assured by the means of the adoption of the safety measures provided for by Decree Law 196/2003. The Adoption of the DPS confirms what here-above and it is here recalled to be integrating part of this Model (at Company’s headquarters);

3. **Creation of “Information Services” Area** with the identification of the Subject responsible for the software customisation activities and for the management of IT procedures. In his/her role of System Administrator, he/she is responsible for the control of physical and logical accesses and of software safety, for guaranteeing the correct management and the constant control of management process and the use of IT systems from the part of the users;
4. **Clear identification of the Subjects that are entrusted with passwords or codes for accessing the IT systems of the Public Administration.** The President or the General Manager are the only people who possess access codes for public offices (such as the PIN number of the Agenzia Entrate, Company Register etc.) and/or for Credit Institutions (for example: access to current accounts by the means of home banking). They can delegate the use of the codes to their subordinates exclusively of the aims related to corporate activities and only expressly for these;
5. **Traceability of the interventions on hardware workplaces and of the modifications made on the IT procedures;**
6. **Traceability of the processes carried out by the means of IT tools** (recording of events such as accounting modifications, variation of users’ profiles, etc. with the log file system);
7. **Provision and clear highlighting of certain behavioural prohibitions and obligations** in this Special Part (Paragraph D.3);
8. **Provision of periodic and constant information flows** addressed to the Supervisory Body (Paragraph D.5 and General Part);
9. **Provision of information and training activities** on the Model (General Part);
Provision of an adequate sanctioning system for the violation of the rules of the Code of Ethics and of the Model (Disciplinary System - General Part)

D.5. Information Flows

The Functions and/or Company's Collaborators involved in the areas at risk as per this Special Part are to promptly warn the Supervisory Body about any violation of this Model and/or of the Code of Conduct.

In particular:

The Person Responsible for the IT Services is the Subject identified by the Company to send the SB an annual report containing information about:

- Damages or faults to the IT systems that cannot be justified with reference to a normal use of the same;
- Inappropriate use of internet and email services;
- Inappropriate use of passwords for the access to IT workstations and/or to access home banking services and/or to access the IT systems of Public Bodies (Agenzia Entrate, CCIAA, etc.), he/she has become aware of;
- Eventual anomalies found in the use of corporate hardware and/or software;
- Eventual litigations, complaints, objections with the companies that supply hosting services.

D.6. Tasks of the Supervisory Body

The SB will have the right to carry out all checks deemed appropriate on every operation considered potentially at risk of committing IT crimes. Written evidence is to be given of the same checks.

Moreover, with the support of the Person Responsible for the IT services and/or other experts, the Supervisory Body is to:

- Verify the observance and the putting into practice of the Model with reference to the notification of the committing of IT crimes;
- Record the behavioural discrepancies that were eventually to arise from the analysis of the IT flows and the received notifications.

**SPECIAL PART E): ORGANISED CRIME OFFENCES
(Criminal Association and Mafia-type Conspiracy)**

E.1. Aim of this Special Part

This Special Part makes reference to forms of behaviour of Company's Employees, Bodies, Consultants and Collaborators operating in favour and on behalf of the Company.

Objective of this Special Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what here-stated, in order to prevent the committing of Organised Crime Offences that EP may theoretically be held responsible for.

In particular, this Special Part has the objective of:

- Detailing the protocols and procedures the Recipients are to respect, to the aims of the correct application of the Model;
- Supplying the operative tools to allow the Supervisory Body and the People Responsible for the other Company's Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities.

Attachment 7 contains the detailed indications of Organised Crime Offences as per art. 24 ter. of the Decree Law 231/2001.

E.2. Areas/Processes at risk and involved Functions

First of all, it is here highlighted that organised crime offences may be any type of crime. As such, they may not be even described in the list of offences provided for by Decree Law 231/2001.

Jurisprudence shows that such forms of behaviour are usually typical of Top Management. Thus, for the peculiarity of the crimes here-discussed, Top Management is to be considered involved *in primis*. This is due to the fact that the creation of forms of organised crime that could benefit the Company may arguably be conceived by those People in possession of all necessary power, skills and contacts. Naturally, even their subordinates can take part to the criminal association.

Criminal forms of behaviour can be extremely varied. For example, criminal association for the purpose of embezzlement (by the means of a system of overcharging or false invoices, involving one or more Senior Managers together with some Suppliers), or operations aimed at the creation of "funds" subsequently destined to corruption activities.

With reference to the crimes stated in attachment 7 and reported from art. 24 ter. of the Decree Law 231/2001, possible crimes may be the following, by way of mere example:

- Organised crime aimed at the committing of fiscal frauds (for example: "carousel" frauds);
- Organised crime aimed at the committing of frauds for the awarding of public financing with reference also to EU projects;
- Participation in a Mafia-style criminal association for the illicit dumping of waste (so-called: "eco-mafias"- DL 152/2006);
- Criminal association with the aim of violating industrial secrets (ex art. 621 Penal Code).

Bearing in mind the here-above examples:

Sensitive Activities	Area/Function	Possible Crimes
Management of financial flows	President, General Manager, Person Responsible for Administration and Personnel, External Consultants	Associated Crime
Management of paperwork for requests/participation in tenders for the awarding of contributions and public funds	President, General Manager, Person Responsible for Administration and Personnel, Person Responsible for the Development of Use and Rules, External Consultants	Associated Crime
Management of integrated system for ELT disposal	President, General Manager District Oversight Functions, Person Responsible for Operations and Logistics, Consultants (Auditors, Lawyers, etc.) and, in any case, all involved Functions	Associated Crime Mafia-Style criminal association
Management of qualified data/know how	President, General Manager, Person Responsible for Administration and Personnel, Person Responsible for IT Services, Consultants	Associated Crime

E.3. General principles of behaviour – Prohibitions and Obligations

Being naturally related to other and different types of offence, crime association may impact also on sensitive areas and processes. These may, from time to time, be involved in the final crime for which the criminal association is supposed to have been created. These sensitive areas and processes have already been dealt with in other Special Parts. In such case, one shall refer to what already provided for in each Special Part.

In general, the Recipients **are strictly expected to:**

- Observe all Rules and Regulations provided for by the Law and internal Company's procedures with reference to the carrying out of normal corporate activities;
- refrain from putting in place, collaborating or giving rise to forms of behaviour that, taken individually or collectively, may integrate the types of offences of organised crime.

E.4. Internal Control System – Specific Procedures

In order to avoid the committing of organised crime offences, the internal control system is necessarily based also on the overall set of corporate protocols, rules, policies and procedures already mentioned in other Special Parts. This is due the fact that, as already repeated several times, organised crime offences may be committed for the most varied criminal aims (crimes-scope).

For the same reason, the preparation of *ad hoc* procedures is quite difficult.

It is here highlighted that, to protect the afore-identified sensitive areas and activities with reference to *financial flows management*, as well as *the paperwork the Public Administration is involved in* and for the *management of qualified data*, it is possible to recall corporate protocols, procedures and policies already expressed in other Special Parts and which the Recipients are to comply with.

ELT disposal integrated management system

For the particular relevance of the activities that integrate ELT management, above all with reference to the phases of collection, storage and subsequent transport towards the disposal platforms, it is here specified that the Company has provided for a number of checks, protocols, policies and operative procedures aimed at preventing and discouraging every form of organised crime in that sensitive area.

1. Code of Ethics

EP's Code of Ethics contains a number of specific principles that make reference to correctness, loyalty and transparency.

2. Clear identification and separation of roles

There is a clear separation of roles between those who have decisional and expenditure power (President and General Manager) and those who operatively carry out the activities inherent the integrated system management, above all, making reference to the *in situ* control of territorial commercial partner companies (transporters, storage companies, cement factories, shredding facilities etc.), namely the four District Oversight Functions divided by territorial area.

3. Technical Audit

A major company with consolidated experience in the sector of corporate controls and certifications chosen by the means of a tender shall perform a number of verifications of the activities carried out by the chain operators in each territory and with reference to the various stages of the ELT disposal chain. This constitutes both a deterrent and a subsequent form of control.

4. Specific Training /communication courses

The Company promotes and organises specific training courses in favour of those Subjects who may find themselves in situations of contact and/or proximity with potential crime associations.

5. Policy-procedure on how the District Oversight Functions are to behave

From the moment that they are located on the territory where they may come in contact with crime associations, the District Oversight Functions are to follow what stated in the policy provided for by the Company. This policy gives indications about how to behave with technical partners and/or members of other companies.

For what concerns their relationship with the local Public Administration, they are to follow the "Procedure for the management of the relationship with the PA".

6. Customised website /workshops and studies

The Company's focus on completely discouraging and repressing crime association is often carried out also by the means of the drafting of documents, researches, social analyses and detailed studies. These are often widely advertised, both internally and externally (also by the means of their publication on the website www.ecopneus.it).

7. Sanctions provided for by the Disciplinary System (General Part)

E.5. Information Flows

All Company's Functions are to promptly notify the Supervisory Body about any form of behaviour, anomaly or irregularity (even documental) that may be evidence of the creation of a crime association or of the participation of EP's Employees and Collaborations in a mafia-style crime association.

E.6. Tasks of the Supervisory Body

The SB will have the right to carry out all checks deemed appropriate on every operation considered potentially at risk of committing crime association offences. Written evidence is to be given of the same checks, thus protecting the privacy of the involved Subjects.

SPECIAL PART F) CRIMES OF RECEIVING OF STOLEN GOODS, OF MONEY-LAUNDERING, OF USE OF MONEY, GOODS AND BENEFITS OF ILLICIT PROVENANCE AS WELL AS CRIMES OF “SELF-LAUNDERING”

F.1. Aim of this Special Part

This Special Part makes reference to forms of behaviour of Company’s Employees and Bodies, as well as its Consultants and Collaborators, as already defined in the General Part.

Objective of this Special Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what provided for by the same Special Part, in order to prevent the committing of the crimes of receiving of stolen goods, of money-laundering, of use of money, goods and benefits of illicit provenance.

In particular, this Special Part has the objective of:

- Detailing the protocols and procedures the Company’s Employees, Bodies, Consultants and Collaborators are to respect, to the aims of the correct application of the Model;
- Supplying the operative tools to allow the Supervisory Body and the People Responsible for the other Company’s Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities.

Attachment 8 contains detailed indications of the Crimes of receiving of stolen goods, money-laundering, of use of money, goods and benefits of illicit provenance as per art. 25 *octies* of the Decree Law. 231/2001.

F.2. Areas and Processes at risk and involved Functions

With reference to the crimes of receiving of stolen goods, of money-laundering, of use of money, goods and benefits of illicit provenance as well as of self-laundering as per art. 25 *octies* of the Decree Law 231/2001, the sensitive activities which are considered mainly at risk are the following:

Sensitive Activities	Area/Function	Possible Crimes
Management of incoming and outgoing financial flows	President; General Manager; Person Resp. Administration Area;	Receiving of stolen goods, money-laundering, use of money, goods and benefits of illicit provenance and self-laundering
Management of contracts	President; General Manager; Person Resp. Administration Area; ; Person Resp. Operations and Logistics	Receiving of stolen goods, money-laundering, use of money, goods and benefits of illicit provenance and self-laundering
In theory, purchasing of productive goods (or linked to corporate activities) coming from thefts/robberies	President; General Manager; Person Resp. Administration Area; ; Person Resp. Operations and Logistic	Receiving of stolen goods
In theory, in case of the committing of a tributary crime, (e.g.: fraudulent statement by the means of the issuing of invoices for non-existing operations), where the profits of fiscal evasion are transferred or used in economic/financial activities (economic legal circuit) so as to prevent the identification of their provenance	President; General Manager; Person Resp. Administration Area; ; Person Resp. Operations and Logistic	Self-laundering

F.3. General principles of behaviour – Specific Procedures

This Special Part expressly **forbids** the Company’s Bodies, Employees and Collaborators **to**:

- put in place, collaborate or give rise to forms of behaviour that, taken individually or collectively, may integrate the afore-identified types of crime;
- Put in place or give rise to violations of Company’s principles and procedures.
- Accept payments and/or money transfers in cash or by cheque.

Moreover, all afore-mentioned Functions involved in the sensitive activities as per this Special Part are **obliged to**:

- Verify the commercial and professional reliability of Suppliers and Business Partners based on relevant indexes (e.g.: public prejudicial data, protests, insolvency procedures or acquisition of commercial information about the Company, its Partners or Administrators);
- Formalise and give documental evidence of the selection process of Suppliers/Technical Partners;
- Formalise the relationship with Suppliers/Technical Partners by the means of the conclusion of contracts in which the clause of the respect of Company’s Code of Ethics is present. This clause is also to provide for the non-respecting of forms of conduct that may integrate the crimes as per DL. 231/2001;

- Verify the economic congruity/proportionality of the purchases/investments with reference to market prices, in order to avoid the risks of recycling committed by the means of apparent accounting anomalies;
- Verify the presence of the necessary documents accompanying the goods entering the Company;
- Employ professionals of high responsibility for sensitive operations;
- Avoid involvements with politically exposed people or with black listed organisations;
- Verify the congruity of payments with reference to the full correspondence between the recipients / payers and the counterparts effectively involved in the transactions;
- Update the assets book and the inventory ledger.

F.4. Internal Control System – Specific Procedures

1. **Adoption of the Code of Ethics**, containing specific behavioural principles also with reference to the collection, aggregation and control of accounting data (Attachment 2);
2. **Adoption of clear and precise identification procedures;**
3. **Prevision and clear highlighting of specific behavioural prohibitions and obligations** in this Special Part (Paragraph F.3);
4. **Adoption of specific Company’s rules and procedures** that define the roles and responsibility of the Functions who transfer money, goods or other benefits.
5. **Company’s rules and procedures**, communicated and/or put at disposal of the Recipients in every office or area involved, are highlighted here below. They are here mentioned as they are integrating and substantial part of this Model:

Management of incoming and outgoing financial flows Administration and statement of accounts	Use of SAP accounting system Use of home banking with secret access codes. The Company is implementing a procedure for purchases
Management of contracts: Management of purchases Management of tenders	Company’s Rule 6 Predetermination of minimum requirements for the offering Subjects: <i>pre</i> and <i>post</i> qualification standards (ref. “Priority requisites for the awarding of supplies”, typical contractual clauses for bidding companies’ requisites, highly specialising requisites requested for participating in EP’s tenders etc.

6. **Implementation of constant and close monitoring with specific reference to incoming and outgoing money flows**, by the means of the adoption of the “SAP” IT system of integrated accounting management. The main characteristic of the SAP software is that it allows to process data in real time. This guarantees essential and transversal functions, such as: the login to the system, the navigability (menu), the parametric personalisation of the components (customising) and many enhancement features.
The control of the financial and accounting processes, thus, are carried out by the means of the aforementioned software, which verifies the correspondence between the purchase order-goods reception and the services-payment-invoicing. Examples of accounting processes carried out with the SAP system may be: general accounting, the definition and updating of the accounts, the entering of petty cash information, the definitions of budgets, of cost centres and of rules of cost distribution.
For what concerns the management of the purchasing orders, the invoicing and the payment systems, there are consolidated corporate procedures which allow crossed checks between those who make the purchasing request (the Person Responsible for each Division), those who authorise it and make the payment (General Manager) and those who carry out the accounting control (Person Responsible for Administration and Personnel) thanks to the division of competences and proxies. In any case, an implementation process of the purchasing management procedure is ongoing (Company’s Rule n 6).
7. **Provision of periodic and constant information flows** addressed to the Supervisory Body (Paragraph F.5 and General Part).
8. **Provision of information and training activities** on the Model (General Part);
9. **Provision of an adequate sanctioning system** for the violation of the rules of the Code of Ethics and of the Model (Disciplinary System - General Part)

F.5. Information Flows

The Functions and/or Company’s Collaborators involved in the areas at risk as per this Special Part are to promptly warn the Supervisory Body about any violation of this Model and/or of the Code of Conduct.

In particular:

The Person Responsible for the Operations and Logistics Area, or a person appointed by him/her, is to send the SB an annual report containing information about:

- The investigations carried out in occasion of the selection of Suppliers for contracts of relevant economic entity and/or for framework agreements;
- Indicators of potential penal risks for sellers/buyers;
- The eventual (motivated) exceptions to the procedures.

The person Responsible for the Administration Area, or a person appointed by him/her, is to send the SB an annual report containing information about:

- Eventual anomalies and irregularities in payment flows;
- Eventual (motivated) exceptions to the rules/procedures provided for.

F.6. Tasks of the Supervisory Body

With the support of the Company's Functions of competence, the Supervisory Body will have the right to carry out all checks deemed appropriate. The SB shall give written evidence of the same checks, thus protecting the confidentiality of the Subjects involved.

**SPECIAL PART G) CRIMES AGAINST INDUSTRY AND COMMERCE
(DISRUPTION OF THE FREEDOM OF TRADE OR INDUSTRY– UNFAIR COMPETITION WITH THREATS AND VIOLENCE)**

G.1. Aim of this Special Part

This Special Part makes reference to forms of behaviour of Company's Employees and Bodies, as well as its Consultants and Collaborators, where applicable.

Objective of this Special Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what here-described, in order to prevent the committing of crimes against Industry and Commerce.

In particular, this Special Part has the objective of:

- Detailing the protocols and procedures the Company's Employees and Bodies, as well as its Consultants and Collaborators (where applicable) are to respect, to the aims of the correct application of the Model;
- Supplying the operative tools to allow the Supervisory Body and the People Responsible for the other Company's Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities.

Attachment 9 contains the detailed indications about Crimes against Trade and Industry as per art. 25 bis.1 of the Decree Law 231/2001.

G.2. Areas/Processes at risk and involved Functions

With reference to the crimes and criminal behaviour described in art. 25 bis 1 of Decree Law 231/2001, the sensitive activities which are considered mainly at risk are the following:

Sensitive Activities	Area/Function	Possible Crimes
Management of relationship with competing companies	President; Administrators; General Manager; Person responsible for Operations & Logistics; Consultants and/or other involved Functions	Disruption of the freedom of trade or industry Unfair competition with threats and violence
Taking part to discussions; working committees in which companies of the sector participate; associations of category; creation of Temporary Joint Ventures	President; Administrators; General Manager; Consultants	Disruption of the freedom of trade or industry Unfair competition with threats and violence

G.3. General principles of behaviour

This Special Part **expressly forbids** Company's Bodies, Employees and Collaborators **to**:

- Put in place, collaborate, or give rise to forms of behaviour that, taken individually or collectively, may integrate the types of crime among the ones mentioned here-above, either directly or indirectly;
- Put into place or give rise to forms of violation of Company's principles and procedures.

In particular, it is **forbidden to**:

- Prevent or disrupt business or trade activities with violence, threats or fraudulent means;
- Keep violent or threatening behaviour in their relationship with Competitors;
- Give false information about EP's services and the services supplied by its business partners with the aim of misleading Third Parties;
- Advertise products and technologies of the Company and of its business Partners in a false and misleading way.

G.4. Internal Control System - Specific Procedures

1. **Adoption of the Code of Ethics**, containing specific behavioural principles about loyalty, correctness and transparency (Attachment 2);
2. **Provision and clear highlighting of certain behavioural prohibitions and obligations** in this Special Part (Paragraph G.3);
3. **Adoption of the Administrators' Self-Discipline Code**. Among the other things, this Code aims also at avoiding situations of conflict of interest and to support Administrators' and Management's correct and transparent behaviour.
4. **Provision of periodic and constant information flows** towards the Supervisory Body (Paragraph G.5 and General Part).
5. **Provision of information and training activities** on the Model (General Part);
6. **Provision of an adequate sanctioning system** for the violation of the rules of the Code of Ethics and of the Model (Disciplinary System - General Part).

G.5. Information Flows

All Company's Functions are to promptly warn the Supervisory Body about any form of behaviour, anomaly or documental irregularity that may be evidence of the committing of one of the crimes provided for in this Special Part.

G.6 Tasks of the Supervisory Body

The Supervisory Body has the right to carry out all checks deemed appropriate. Written evidence is to be given of the same checks. The privacy of the Subjects involved is to be protected.

SPECIAL PART H): INSTIGATION NOT TO TESTIFY OR TO BEAR FALSE TESTIMONY TO THE JUDICIAL AUTHORITY

H.1. Aim of this Special Part

This Special Part makes reference to forms of behaviour of Company's Employees and Bodies, as well as its Consultants and Collaborators, where applicable.

Objective of this Special Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what here-described, in order to prevent the committing of the crime of *instigation not to testify or to bear false testimony to the Judicial Authority*

In particular, this Special Part has the objective of:

- Detailing the protocols and procedures the Company's Employees and Bodies, as well as its Consultants and Collaborators (where applicable) are to respect, to the aims of the correct application of the Model;
- Supplying the operative tools to allow the Supervisory Body and the People Responsible for the other Company's Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities.

Attachment 10 contains the indications of the present case as per art. 25 *decies* of the Decree Law 231/2001.

H.2. Areas/Processes at risk and involved Functions

With reference to the crimes and criminal behaviour described in attachment 10 and required by art. 25 *decies* of the Decree Law 231/01, the sensitive activity which is considered more specifically at risk is:

- The management of relationships with Subjects involved in Legal Proceedings.

Sensitive Activities	Area/Function
Relationships with Subjects involved in Legal Proceedings	President and Administrators; General Manager; District Oversight Functions; Person Responsible for Administration and Personnel; Person responsible for Operations & Logistics; Consultants and any other Function aware of the Legal Proceedings

H.3. General principles of behaviour

This Special Part **expressly forbids** Company's Bodies (and its Employees and Consultants/Collaborators to the extent necessary for the accomplishment of their tasks) **to**:

- Put in place, collaborate, or give rise to forms of behaviour that, taken individually or collectively, may integrate the types of crimes as per art. 377 *bis* of the Penal Code;
- Put into place or give rise to forms of violation of Company's principles and procedures.

In particular, it is **forbidden to**:

- Discuss the content of investigation activities being currently carried out by the Public Authorities with the Subjects involved in legal proceedings;
- Instigate those who are called to make statements to the Legal Authority that may be used in legal proceedings not to testify or to bear false testimony – in case they have the right to silence.

In general, the Functions involved in the afore-described sensitive processes **are to respect the following protocols**:

- Respect investigation secrecy during legal proceedings;
- Respect the freedom and autonomy of decision of the Subjects involved in legal proceedings, when these may be asked to bear testimony that may be used as evidence.

H.4. Internal Control System

1. **Adoption of the Code of Ethics**, containing specific behavioural principles about loyalty, correctness, transparency, confidentiality and privacy protection (Attachment 2);
2. **Provision and clear highlighting of certain behavioural prohibitions and obligations** in this Special Part (Paragraph H.3);
3. **Adoption of the Administrators' Self-Discipline Code**. Among the other things, this Code aims also at supporting Administrators' and Management's correct forms of behaviour
4. **Provision of periodic and constant information flows** towards the Supervisory Body (Paragraph H.5 and General Part).
5. **Provision of information and training activities** on the Model (General Part);

6. **Provision of an adequate sanctioning system** for the violation of the rules of the Code of Ethics and of the Model (Disciplinary System - General Part).

H.5. Information Flows and Tasks of the Supervisory Body

All Company's Functions are to promptly warn the Supervisory Body about any form of behaviour, anomaly or documental irregularity that may be evidence of the violation of the obligations of confidentiality and secrecy on any pending legal proceedings and the ongoing investigations.

In order to prevent the committing of the crime provided for in this Special Part, the Supervisory Body has the right to carry out all checks deemed appropriate. Written evidence is to be given of the same checks. The privacy of the Subjects involved is to be protected.

SPECIAL PART I): ENVIRONMENTAL CRIMES

I.1. Aim of this Special Part

This Special Part makes reference to forms of behaviour of Company's Employees and Bodies, as well as its Consultants and Collaborators who act to the advantage of and on behalf of the Company .

Objective of this Special Part is that all its Recipients, as here-above described, adopt rules of conduct in agreement with what here-described, in order to prevent the committing of Environmental Crimes that EP may theoretically be held responsible for .

In particular, this Special Part has the objective of:

- Detailing the protocols and procedures the Recipients are to respect, to the aims of the correct application of the Model;

Supplying the operative tools to allow the Supervisory Body and the People Responsible for the other Company's Functions cooperating with the SB to carry out the planned control, monitoring, and verification activities

Attachment 11 contains the detailed indications of the present case as per art. 25 *undecies* of the Decree Law 231/2001

I.2. Areas/Processes at risk and involved Functions

With reference to the crimes and criminal behaviour described in attachment 11 and required by art. 25 *undecies* of the Decree Law 231/01, the sensitive activities which are considered more specifically at risk are:

Sensitive Activities	Area/Function	Possible Crimes
Operations that may be traced back to Chain activities	- Area Oversight - Companies of the Ecopneus Chain	<i>(Unlawful involvement in)</i> industrial wastewater discharge containing dangerous substances; discharge on ground, underground and in ground water; water discharge in the sea from the part of ships and planes; unintentional crimes against the environment
Management of contracts with third-party companies for the collection, transport and valorisation activities of ELTs.	- Operations and Logistics - Area Oversight - Companies of the Ecopneus Chain	<i>(unlawful involvement in)</i> activities of non-authorized management, transport, recovery, disposal, trade and intermediation of (dangerous and non-dangerous) waste without specific authorisation, registration of communication as per articles 208, 209, 210, 211, 212, 214, 215 e 216 (Single Authorisation)
Temporary waste storage	- Operations and Logistics - Area Oversight - (Technical Audit) - Companies of the Ecopneus Chain	<i>(unlawful involvement in)</i> activities of non-authorized waste management: creation of unauthorised landfills by the means of dumping in unauthorised areas
Treatment, shredding and valorisation of ELTs	- Operations and Logistics - Area Oversight (Technical Audit) - Companies of the Ecopneus Chain	<i>(unlawful involvement in)</i> activities of unauthorised waste management: in violation of art. 187 (prohibition of mixing of dangerous waste types), carrying out of non-allowed activities of waste mixing; unintentional crimes against the environment
Disposal of ELTs within the scope of decontamination projects promoted by the Public Administration or storage carried out on free ground	- Operations and Logistics - Area Oversight - (Technical Audit) - Companies of the Ecopneus Chain	<i>(unlawful involvement in)</i> pollution of soil, subsoil, superficial or underground water; pollution during decontamination activities
Management of copies of MUD (Single Model of Environmental Declaration) or of the forms about the collection and transportation of ELTs prepared by the Operators entrusted with the collection services	- Operations and Logistics - Area Oversight - (Technical Audit) - Companies of the Ecopneus Chain	<i>(unlawful involvement in)</i> violation of the obligations of communication, and of the keeping of the obligatory books and forms
Management of transport to or from shredding and/or valorisation centres	- Operations and Logistics - Area Oversight (Technical Audit)	<i>(unlawful involvement in)</i> waste trafficking. Organised activities for unlawful waste trafficking; unintentional crimes against the environment

	- Companies of the Ecopneus Chain	
Supply of ELTs, or during ELT treatment phases, non-compliant with the certifications issued to the companies of the EP chain	- Operations and Logistics - Area Oversight (Technical Audit) - Companies of the Ecopneus Chain	(<i>unlawful involvement in</i>) Emissions: violation of the limits set or imposed by the authorisations; unintentional crimes against the environment

1.3. General principles of behaviour – Prohibitions and Obligations

The following behavioural principles of general nature are applied to the Recipients of this Model who, for whatever reason, are involved in Company's "sensitive" activities with reference to Environmental Crimes, either directly or indirectly. In particular, these principles apply to all those people who operate with the involvement and the support of the EP chain.

In general, such Subjects **are to**:

- scrupulously respect all Rules and Regulations set out by the Law and the internal Company's procedures and Regulations with reference to the execution of the activities that are sensitive to the potential committing of an environmental crime (or simple involvement in the same);
- refrain from putting in place, collaborate or give rise to forms of behaviour that, taken individually or collectively, may integrate the types of environmental crimes .

Moreover, all Functions involved in the sensitive activities as per this Special Part **are obliged to**:

- verify the trade and professional reliability of the suppliers and business partners of the EP chain. This shall be done even by the means of the control of the possession of the authorisations and the requisites provided for by the Legislation of reference for what concerns environmental crimes, for the supply of the services subject of the contract. This is to guarantee that the execution of such services comply with the legislation of reference;
- formalise the relationship with the Subjects of the EP chain by the means of the signing of contracts possessing the clause of the respect of the Company's Management and Organisation Model and Code of Ethics. This clause shall also provide for the keeping of forms of conduct that may integrate the crimes as per DL 231/2001
- keep and file the documentation of competence produced electronically in order to be able to reconstruct the responsibilities and the choices made;
- verify the completeness of the data necessary in the forms and, more in general, of the documentation accompanying the ELTs along their transformation, valorisation and treatment chain.
- provide for a periodic check of the modalities of evaluation and monitoring of the requisites and of the necessary authorisations provided for by the legislation with reference to Subjects/Suppliers of the chain, who have been entrusted with the services subject of a contract;
- provide for monitoring and, eventually, internal revision of the collection, storage, transport, working and separation methods of the produced waste;
- provide for internal rules and regulations that adopt the rules and regulations provided for by the Legislation in force with reference to the environment and that can be applied to the Company, with the aim of highlighting obligations, limits and prohibitions to be respected .

1.4. Internal Control Systems

1. **Adoption of the Code of Ethics**, containing specific behavioural principles about loyalty, correctness, transparency, confidentiality and privacy protection (Attachment 2)
2. **Provision and clear highlighting of certain behavioural prohibitions and obligations** in this Special Part (Paragraph 1.3)
3. **Adoption of the Administrators' Self-Discipline Code**. Among the other things, this Code aims also at supporting Administrators' and Management's correct forms of behaviour
4. **Provision of periodic and constant information flows** towards the Supervisory Body (Paragraph 1.5 and General Part)
5. **Provision of information and training activities** on the Model (General Part);
6. **Provision of an adequate sanctioning system** for the violation of the rules of the Code of Ethics and of the Model (Disciplinary System - General Part)

I.5. Information Flows

All Company's Functions are to promptly warn the Supervisory Body about any suspect or anomalous form of behaviour that may be evidence of the committing of environmental crimes.

In particular:

The Person Responsible of the Operations and Logistics Area, or a person nominated by the same, is to transmit an annual report to the Supervisory Body. This report is to contain:

- the investigations carried out in occasion of the selection of suppliers for contracts of substantial financial value and/or for framework agreements;
- indicators of potential penal risks sellers/purchasers may suffer ;
- the eventual (motivated) exceptions to the procedures provided for.

I.6. Tasks of the Supervisory Body

In order to prevent the committing of the crime provided for in this Special Part, the Supervisory Body has the right to carry out all checks deemed appropriate. Written evidence is to be given of the same checks. The privacy of the Subjects involved is to be protected.