

RENANTIS SPA

**ORGANISATION AND
MANAGEMENT MODEL
PURSUANT TO
LEGISLATIVE DECREE 231/2001**

Date of approval by the Board of Directors: **15 November 2022**

GENERAL PART

- 1. INTRODUCTION 10**
 - 1.1 Definitions 10
 - 1.2 The administrative liability framework regarding entities 11
 - 1.2.1. Characteristics and nature of entities' liability 11
 - 1.2.2. Criminal offences identified by the Decree and by subsequent amendments 12
 - 1.2.3. Criteria for attributing responsibility to the entity 14
 - 1.2.4. Information in the Decree on the characteristics of the organisation and management model 16
 - 1.2.5. Crimes committed abroad 17
 - 1.2.6. Penalties 18
 - 1.2.7. Events modifying the entity 20
- 2. RENANTIS SPA: THE COMPANY AND ITS INTERNAL CONTROL SYSTEM 22**
- 3. THE MODEL 24**
 - 3.1 Structure of this document 24
 - 3.2 Purposes of the Model 24
 - 3.3 Model and Code of Ethics 25
 - 3.4. Model of the subsidiaries of Renantis S.p.A..... 26
- 4. THE ADOPTION OF THE MODEL 28**
 - 4.1 Methodology for implementing the Model 28
 - 4.2 Changes and updates to the Model 29
 - 4.3 Crimes applicable to the Company 29
 - 4.4 Exposed Individuals under the Model 30
- 5. SUPERVISORY BODY 32**

| | | |
|-----------|---|-----------|
| 5.1 | Function | 32 |
| 5.2 | Requirements and composition of the Supervisory Body | 32 |
| 5.3 | Eligibility and integrity requirements..... | 35 |
| 5.4 | Appointment, removal, replacement, loss of office and resignation | 36 |
| 5.5 | Remuneration of the Supervisory Body | 38 |
| 5.6 | Functions and powers..... | 38 |
| 5.7 | Supervisory Body information flows to the company bodies | 40 |
| 5.8 | Information flows to the Supervisory Body | 42 |
| 6. | PROVISION BY THIRD PARTIES..... | 45 |
| 7. | INTERCOMPANY SERVICE CONTRACTS..... | 46 |
| 8. | DISCIPLINARY SYSTEM | 47 |
| 8.1 | General principles | 47 |
| 8.2 | Penalties against Employees/ Collaborators with an employment contract | 48 |
| 8.3 | Measures against Directors | 51 |
| 8.4 | Measures against members of the Supervisory Body | 51 |
| | Measures against Third Parties | 52 |
| 9. | COMMUNICATION AND TRAINING OF COMPANY PERSONNEL | 53 |
| | SPECIAL PART | 54 |
| 1. | INTRODUCTION | 54 |
| 2. | GENERAL RULES OF CONDUCT..... | 54 |
| 3. | GENERAL PREVENTION PROTOCOLS..... | 54 |
| 4. | INTERCOMPANY SERVICE CONTRACTS..... | 56 |

| | | |
|------------|--|------------|
| A. | OFFENCES COMMITTED IN RELATIONS WITH THE PUBLIC ADMINISTRATION (ARTICLES 24 AND 25 OF THE DECREE) | 57 |
| A.1 | Introduction | 57 |
| A.2 | Applicable offences | 58 |
| A.3 | Sensitive Activity..... | 62 |
| A.4 | Specific prevention protocols..... | 63 |
| B. | COMPUTER CRIMES AND UNLAWFUL DATA PROCESSING (ARTICLE 24-BIS OF THE DECREE) | 87 |
| B.1 | Applicable offences | 87 |
| B.2 | Sensitive Activity | 89 |
| B.3 | Specific prevention protocols and respective implementation..... | 89 |
| C. | ORGANISED CRIME AND TRANSNATIONAL OFFENCES (ARTICLE 24-TER OF THE DECREE AND ARTICLE 10, ITALIAN LAW NO. 146 OF 16 MARCH 2006.) | 94 |
| C.1 | Applicable offences | 94 |
| C.2 | Sensitive Activity | 95 |
| C.3 | Specific prevention protocols..... | 97 |
| D. | CRIMES AGAINST INDUSTRY AND TRADE (ARTICLE 25-BIS.1 OF THE DECREE) | 99 |
| D.1 | Applicable offences | 99 |
| D.2 | Sensitive Activity | 99 |
| D.3 | Specific prevention protocols..... | 99 |
| D.4 | Implementation of specific prevention protocols..... | 100 |
| E. | CORPORATE OFFENCES (ARTICLE 25-TER OF THE DECREE) | 101 |

| | | |
|-----------|--|------------|
| E.1 | Applicable offences | 101 |
| E.2 | Sensitive Activity | 103 |
| E.3 | Specific prevention protocols | 104 |
| F. | CRIMES AGAINST THE INDIVIDUAL (ARTICLE 25-QUINQUIES OF THE DECREE)..... | 112 |
| F.1. | Applicable offences | 112 |
| F.2 | Sensitive Activity | 113 |
| F.3 | Specific prevention protocols | 113 |
| G. | CULPABLE HOMICIDE OR GRIEVOUS OR VERY GRIEVOUS HARM COMMITTED IN VIOLATION OF THE RULES ON PROTECTION OF HEALTH AND SAFETY AT WORK (ART. 25-SEPTIES OF THE DECREE)..... | 114 |
| G.1 | Applicable offences | 114 |
| G.2 | Sensitive Activity | 116 |
| G.2.1. | Introduction | 116 |
| G.2.2. | Sensitive Activity | 117 |
| G.3. | General rules of conduct | 119 |
| G.4. | Specific prevention protocols | 121 |
| G.5. | Additional checks | 129 |
| G.6. | Audit activity for the periodic check of the application and effectiveness of the procedures of the specific prevention protocols..... | 133 |
| G.7. | Implementation of specific prevention protocols | 134 |
| H. | RECEIVING STOLEN GOODS, MONEY LAUNDERING AND USE OF MONEY, GOODS OR BENEFITS OF UNLAWFUL ORIGIN, AS WELL AS SELF-MONEY LAUNDERING (ARTICLE 25-OCTIES OF THE DECREE) . | 135 |
| H.1 | Applicable offences | 135 |

| | | |
|-----------|--|------------|
| H.2. | Sensitive Activity | 135 |
| H.3. | Specific prevention protocols | 136 |
| H.4. | Reporting of transactions/ operations considered potentially at risk in terms of “self-money laundering” | 139 |
| I. | CRIMES RELATING TO COPYRIGHT VIOLATION (ARTICLE 25-NOVIES OF THE DECREE)..... | 141 |
| I.1 | Applicable offences..... | 141 |
| I.2 | Sensitive Activity | 141 |
| I.3. | General principles of behaviour | 141 |
| I.4 | Specific prevention protocols and respective implementation..... | 142 |
| J. | INCITEMENT NOT TO MAKE STATEMENTS OR TO MAKE FALSE STATEMENTS IN COURT (ART. 25-DECIES OF THE DECREE) | 144 |
| J.1. | Applicable offence..... | 144 |
| J.2. | Sensitive Activity | 144 |
| J.3. | Specific prevention protocols and respective implementation | 144 |
| K. | ENVIRONMENTAL OFFENCES (ART. 25-UNDECIES OF THE DECREE) 145 | |
| K.1. | Introduction | 145 |
| K.2. | Applicable offences | 145 |
| K.3. | Sensitive Activity | 146 |
| K.4. | General rules of conduct..... | 146 |
| K.5. | Specific prevention protocols | 147 |
| K.6. | Audit activity for the periodic check of the application of the specific prevention protocols | 150 |
| K.7. | Implementation of specific prevention protocols | 150 |

| | |
|---|------------|
| L. CORRUPTION IN THE PRIVATE SECTOR (INCLUDED AMONG THE CORPORATE OFFENCES REFERRED TO IN ARTICLE 25-TER OF THE DECREE)..... | 152 |
| L.1. Applicable offences | 152 |
| L.2. Sensitive Activity | 152 |
| L.3. General rules of conduct | 153 |
| L.4. Specific prevention protocols | 154 |
| M. EMPLOYMENT OF ILLEGALLY STAYING THIRD-COUNTRY NATIONALS (ARTICLE 25-DUODECIES OF THE DECREE)..... | 156 |
| M.1. Applicable offences | 156 |
| M.2. Sensitive Activity | 156 |
| M.3. Specific prevention protocols | 156 |
| N. TAX CRIMES (ART. 25-QUINQUIESDECIES OF THE DECREE)..... | 157 |
| N. 1. Applicable offences | 157 |
| N. 2. Sensitive Activity | 159 |
| N. 3. General rules of conduct | 160 |
| N. 4. Specific prevention protocols | 161 |
| O. OFFENCES RELATING TO NON-CASH PAYMENT INSTRUMENTS (ART. 25-OCTIES.1 OF THE DECREE); | 168 |
| O.1. Applicable offences | 168 |
| O.2. Sensitive Activity | 169 |
| O.3. Specific prevention protocols | 169 |
| P. CRIMES AGAINST CULTURAL HERITAGE (ARTS. 25-SEPTIESDECIES AND 25-DUODEVICIES OF THE DECREE)..... | 171 |

| | | |
|------|-------------------------------------|-----|
| P.1. | Applicable offences | 171 |
| P.2. | Sensitive Activity | 171 |
| P.3. | Specific prevention protocols | 172 |

MODEL REVISIONS

| Adoption of Model | Update of Model | Date of Board of Directors resolution |
|-------------------|-----------------|---------------------------------------|
| 10 JUNE 2004 | | |
| | ✓ | 12 MAY 2006 |
| | ✓ | 14 FEBRUARY 2008 |
| | ✓ | 7 MAY 2009 |
| | ✓ | 22 DECEMBER 2009 |
| | ✓ | 13 MAY 2011 |
| | ✓ | 24 JULY 2012 |
| | ✓ | 23 JULY 2013 |
| | ✓ | 10 DECEMBER 2014 |
| | ✓ | 28 APRIL 2016 |
| | ✓ | 13 APRIL 2017 |
| | ✓ | 21 SEPTEMBER 2017 |
| | ✓ | 31 JULY 2018 |
| | ✓ | 30 JULY 2019 |
| | ✓ | 03 DECEMBER 2020 |
| | ✓ | 23 JUNE 2021 |
| | ✓ | 15 NOVEMBER 2022 |

GENERAL PART

1. INTRODUCTION

1.1 Definitions

“ **Sensitive Activity** ”: activities of the Company within the scope of which there is the risk, even if potential, of the commission of crimes as per the Decree.

“ **CCNL** ”: National Collective Labour Agreement currently in effect applied by the Company.

“ **Code of Ethics** ”: code of conduct adopted by the Group.

“ **Employees/ Collaborators** ”: parties with an employment or quasi self-employment contract with the Company or who operate through a staffing agreement, who work, even if partially, at the workplaces of the Company or whose work is nevertheless coordinated with the company organisation such as to allow the Company to engage in preventive oversight on the commission of predicate offences.

“ **Legislative Decree no. 231/2001** ” or “ **Decree** ”: Italian Legislative Decree no. 231 of 8 June 2001 concerning the “Regulations governing the administrative liability of legal entities, companies and associations, even without legal status pursuant to art. 11 of Law no. 300 of 29 September 2000” as subsequently amended and modified.

“ **Company Representatives** ”: directors, statutory auditors, liquidators and Employees/Collaborators.

“ **Suppliers** ”: suppliers of goods and providers of services, whether of an intellectual nature or not, not connected to the Company through employment, including consultants.

“ **Group** ”: collectively the companies controlled by Renantis S.p.A., including the Company.

“ **Public Service Appointee** ”: anyone who for any reason provides a “public service”, to be understood as an activity governed in the same way as civil service, but characterised by the lack of powers typical thereto pursuant to art. 358, Criminal Code.

“ **Model** ”: organisation and management model established by art. 6 of Legislative Decree no. 231/2001.

“ **Corporate Bodies** ”: Board of Directors and Management Control Committee of the Company and their members.

“Supervisory Body” or **“SB”**: Body established by Article 6 of the Decree, in charge of supervising the operation and compliance with the Model as well as of updating it.

“PA”: Public Administration.

“Partner”: natural persons or legal entities, with which the Company has a commercial cooperation relationship governed under agreement (temporary consortium, joint venture, consortium, license, agency, collaboration in general).

“Public Officer”: anyone in a public sector position in the legislative, judicial or executive branches pursuant to art. 357, Criminal Code.

“Company”: Renantis S.p.A.

“Senior individuals”: persons holding positions for which they represent, manage or direct the Company or a unit thereof possessing financial and functional autonomy, as well as persons engaged, even on a de facto basis, in the management or supervision of the Company.

“Subordinate Individuals”: persons subject to the management or supervision of Senior individuals.

“Model implementation instruments”: all provisions, internal orders, documents and Group operational procedures, etc., such as articles of association, delegations and powers, organisational charts, procedures and organisational provisions.

Corporate Unit(s): organisational units of the Company or other Group companies, through which the Company pursues the achievement of its corporate purpose.

“Third Parties”: Partners, Suppliers and more in general those collaborating with the Company, although not connected by an employment, quasi self-employment or supply contract.

“TUF”: Legislative Decree no. 58 of 24 February 1998, so-called Consolidated Act on Financial Intermediation, as subsequently amended and modified.

1.2 The administrative liability framework regarding entities

1.2.1. Characteristics and nature of entities’ liability

On implementing international anti-corruption legislation, the Decree introduces and governs the administrative liability of collective entities, resulting from crime. It is a new form of liability since up until 2001 such entities could only be compelled to pay, on a joint and several basis, fines, financial penalties and administrative sanctions imposed upon respective legal representatives, directors or Employees/Collaborators.

The nature of this new form of liability is “mixed” and its distinctive feature is that it combines aspects of the system of criminal and administrative penalties. In fact, based on the Decree the entity is punished with a penalty of an administrative nature, insomuch as it answers for an administrative offence, but the system of penalties is based on criminal procedure: the authority responsible for bringing charges on the offence is the public prosecution service, and it is a criminal judge that issues the penalty.

An entity’s administrative liability is different and independent with respect to that of the natural person who commits the crime and it exists even if the perpetrator of the crime has not been identified, or when the crime is extinguished for a reason other than amnesty. In any case, the liability of an entity must always be added to and never replace that of the natural person who perpetrated the crime.

The scope of application of the Decree is very wide-ranging and concerns all entities with legal status, companies, associations (even if without legal status), state-controlled firms and private entities that are the licensees of a public service. On the other hand, the legislation is not applicable to the State, to regional and local authorities, to non-profit state-controlled entities and to entities holding roles of constitutional importance (such as, for example, political parties and trade unions).

The legislation does not refer to entities without a branch in Italy. In any case, in this regard, basing the decision on the territoriality principle, case law has established that Italian courts have jurisdiction over crimes committed by foreign entities in Italy.

1.2.2. Criminal offences identified by the Decree and by subsequent amendments

An entity may be called upon to answer for only the crimes indicated by the Decree – so-called predicate offences – or in any case by a law effective before the commission of the act constituting a crime.

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

- offences committed in relations with the Public Administration (arts. 24 and 25 of the Decree);
- computer crimes and unlawful data processing (article 24-bis of the Decree);
- organised crime (article 24-ter of the Decree);
- counterfeiting crimes involving money, legal tender, revenue stamps and instruments or distinguishing marks (art. 25-bis of the Decree);
- crimes against industry and trade (article 25-bis.1 of the Decree);
- corporate offences (article 25-ter of the Decree);
- corruption in the private sector and incitement to corruption in the private sector (included among the crimes under art. 25-ter of the Decree);
- offences for terrorism purposes or for the overthrow of democracy (art. 25-quater of the Decree);
- female genital mutilation crimes (art. 25-quater.1 of the Decree);
- crimes against the individual (article 25-quinquies of the Decree);
- administrative market abuse crimes and offences (art. 25-sexies of the Decree, as well as articles 187-bis, 187-ter and 187-quinquies of the TUF);
- crimes of culpable homicide or grievous or very grievous harm committed in violation of the rules on protection of health and safety at work (art. 25-septies of the Decree);
- crimes of receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-money laundering (art. 25-octies of the Decree);
- offences relating to non-cash payment instruments (art. 25-octies.1 of the Decree);
- crimes relating to copyright violation (article 25-novies of the Decree);

- incitement not to make statements or to make false statements in court (art. 25-decies of the Decree);
- environmental offences (art. 25-undecies of the Decree);
- employment of illegally staying third-country nationals (article 25-duodecies of the Decree);
- racism and xenophobia (art. 25-terdecies of the Decree);
- crimes of fraud in sports competitions and unauthorised involvement gaming or betting activities (art. 25-quaterdecies of the Decree);
- transnational crimes (art. 10 Law no. 146 of 16 March 2006 of the Decree);
- tax crimes (art. 25- quinquiesdecies of the Decree);
- smuggling crimes (art. 25-sexiesdecies of the Decree);
- crimes against cultural heritage (arts. 25-septiesdecies and 25-duodevicies of the Decree).

The applicability and the relevance of each crime for the Company is analysed in depth in section 4.3 of this General Part.

1.2.3. Criteria for attributing responsibility to the entity

In addition to the commission of one of the predicate offences, in order that the entity may be subject to penalties pursuant to the Decree, the criteria identified by lawmakers must be met. Said further criteria may be distinguished as “objective” and “subjective”.

The first objective criterion is made up of the fact that the crime must have been committed by an individual connected to the entity by a qualified relationship. In this regard, one distinguishes between:

- Senior individuals – these are persons who actually have an independent power to make decisions in the name of and on behalf of the entity. Furthermore, all individuals delegated by directors to engage in management or supervision of the entity or of its branch offices may be included in this category;

- Subordinate Individuals – Employees/Collaborators and all parties who, although not part of the staff, work under the supervision and oversight of Senior individuals or in any case undertake an activity in the name of, on behalf of or in the interest of the entity itself belong to this category.

Another objective criterion is represented by the fact that the offence must be committed in the interest or to the advantage of the entity; the existence of at least one of the two alternative conditions is sufficient:

- the interest exists when the perpetrator of the offence has acted with the intention of favouring the entity, regardless of the circumstance that this objective has actually been achieved;
- there is a benefit when the entity obtained a positive financial or other result from the crime.

The concepts of interest and benefits must not be understood as a single concept, but rather separate ones, as there is an obvious distinction between what may be understood as a possible gain foreseen as a consequence of the offence, with respect to the benefit clearly achieved due to the outcome of the crime. The two criteria for determining interest and benefit are alternatives to each other.

The entity is liable not only when it obtained an immediate pecuniary benefit from the commission of the crime, but also in the event that, even in the absence of such result, the act is motivated by the entity's interest. The improvement of its position in the market or the concealment of a situation of financial crisis, for example, are cases that involve the entity's interests without, however, bringing it an immediate financial benefit.

As to the subjective criteria for attributing a crime to the entity, they relate to preventive tools possessed by it to prevent the commission of one of the crimes established by the Decree in the company's operations.

- In fact, the Decree establishes that the entity is to be removed from responsibility only if it demonstrates: that the managing body adopted and effectively implemented, before

commission of the act, organisational, management and control models capable of preventing crimes of the sort discovered;

- that the task of supervising the operation and observance of the models and to oversee their updating was assigned to a body of the entity possessing independent powers of action and supervision;
- that supervision by the aforementioned body was not omissive or insufficient.

The conditions just listed must all be met in order to remove the entity from responsibility. Notwithstanding that the model acts as a reason for non-punishability, whether the predicate offence was committed by a person in a senior position, or committed by a person in a subordinate position, the mechanism established by the Decree regarding the burden of proof is much more uncompromising for the entity in the event that the crime was committed by a person in a senior position. In the latter case, in fact, the entity must demonstrate that the persons committed the crime by fraudulently circumventing the model; the Decree therefore requires stronger proof of non-involvement, insomuch as the entity must also prove fraudulent conduct by Senior individuals.

In the case of crimes committed by individuals in a subordinate position, the entity may instead be called upon to answer only if it is ascertained that commission of the crime was made possible by non-observance of supervision or management obligations. In any case, it is ruled out if, before commission of the crime, the entity possessed an organisation and management model capable of preventing crimes of the sort committed. In this case, one is faced with real negligence in organisation: the entity indirectly allowed commission of the crime, by not supervising actions or conduct of individuals at risk of committing a predicate offence.

1.2.4. Information in the Decree on the characteristics of the organisation and management model

The Decree just governs certain general principles concerning the organisation and management model, without however providing specific characteristics. The model only acts as a reason for non-punishability if:

- effective, that is, if reasonably capable of preventing the committed crime or crimes;
- effectively implemented or if its content is applied in the corporate procedures and in the internal control system.

As to the effectiveness of the model, the Decree establishes that it must have the following minimum content:

- identification of the entity's activities within the scope of which crimes may be committed;
- establishment of specific procedures aimed at planning the formation and implementation of entity decisions, in relation to the crimes to be prevented;
- identification of the procedures for managing financial resources capable of preventing the commission of crimes;
- introduction of a disciplinary system capable of penalising non-compliance with the measures indicated in the model;
- establishment of disclosure obligations with respect to the Supervisory Body;
- in relation to the nature and size of the organisation, as well as to the type of operations, establishment of measures capable of ensuring operations in compliance with the law and of discovering and eliminating in a timely manner situations of risk that may involve the commission of a crime under the Decree.

The Decree establishes that the Model must be checked periodically and updated, either in the event that significant violations of the provisions come to light, or if there are significant changes to the organisation or operations of the entity or modifications in the legislation of reference, in particular when new predicate offences are introduced.

1.2.5. Crimes committed abroad

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

Nevertheless, the Decree subjects this possibility to the following conditions, which are obviously in addition to those already highlighted:

- satisfaction of the general conditions for prosecutability as established in arts. 7, 8, 9 and 10 of the criminal code in order to prosecute in Italy a crime committed abroad;
- the entity has its main headquarters in Italy;
- the country where the crime was committed has not prosecuted the entity.

1.2.6. Penalties

The penalty system envisaged by Italian Legislative Decree 231/2001 is divided into four types of penalties to which the entity may be subject in the event of conviction pursuant to the Decree:

- pecuniary penalty: this is always applied if the judge holds the entity responsible. It is calculated by way of a system based on quotas, which are determined by the judge as to the number and amount: the number of the quotas, to be applied between a minimum and a maximum varying according to the circumstances, depends on the seriousness of the crime, on the degree of responsibility of the entity, on the actions taken to eliminate or attenuate the crime's consequences or to prevent the commission of other unlawful acts; the amount of the individual quota must instead be established depending on the financial and economic situation of the entity;
- prohibiting penalties: prohibiting penalties apply, in addition to pecuniary penalties, only if expressly established for the crime for which the entity is convicted and only in the event that at least one of the following conditions is met:
 - the entity obtained a significant benefit from the crime and the crime was committed by a Senior Individual, or by a Subordinate Individual if the commission of the crime was made possible by serious organisational deficiencies;
 - in the event of the repetition of unlawful acts.

The prohibiting penalties established by the Decree are:

- debarment from an activity;
- suspension or revocation of the authorisations, licenses or allowances functional to the commission of the offence;
- ban on entering into contract with the Public Administration, except to obtain the provision of a public service;
- exclusion from benefits, financing, contributions or subsidies and any revocation of that already granted;
- ban on publicising goods or services.

Exceptionally applicable on a definitive basis, prohibiting penalties are temporary and concern the specific activity of the entity to which the unlawful act refers. They may also be applied on a pre-trial basis, before the conviction, at the request of the Public Prosecution Service, if there is strong evidence of the entity's responsibility and well-founded and specific information leading to believe that there is a concrete danger of further commission of unlawful acts of the same sort as those being prosecuted;

- seizure: with a conviction, there is always an order to seize the value or profit from the crime either in goods or other benefits of equivalent value. The profit earned from the offence was defined by case law as the economic advantage of direct and immediate causal derivation from the offence and concretely determined net of the actual benefit achieved by the victim in any contractual relationship with the entity; based on this definition, one must exclude any business parameter, so the profit cannot be identified with the net profit achieved by the entity (except in the case normally envisaged of administration through an external commissioner). In addition, non-decrease in assets caused by non-disbursement of sums for costs that should have been incurred is not to be considered as extraneous to the concept of profit;
- publication of the conviction: this may be ordered when a prohibiting penalty is imposed upon the entity. It consists of the publication of the conviction once, as an excerpt or in full, in one or more newspapers indicated by the judge in the judgement or by posting in the Municipality where the entity has its main headquarters.

The final conviction of the entity is entered in the national registry of administrative penalties for offence.

1.2.7. Events modifying the entity

The Decree regulates the liability system of the entity in case of transformation, merger, demerger and transfer of the company.

In the event of conversion of the entity, it retains responsibility for the crimes committed prior to the conversion effective date. The new entity will therefore be subject to the penalties applicable to the original entity, due to facts committed prior to the conversion.

In the event of merger, the entity resulting from the merger itself, including due to takeover, answers for the crimes for which the entities that participated in the merger were responsible. If it took place before the conclusion of the assessment of the entity's liability, the Court must take into account the economic conditions of the original entity and not those of the entity resulting from the merger.

In the event of demerger, the demerged entity retains responsibility for the crimes committed before that date on which the demerger took effect. The beneficiary entities of the demerger are liable on a joint and several basis for the payment of pecuniary penalties imposed upon the demerged entity up to the limits of the net equity transferred to each individual entity, unless dealing with an entity to which the business unit within the scope of which the crime was committed was transferred also in part; prohibiting penalties apply to the entity (or to the entities) remaining with or receiving the business unit within the scope of which the crime was committed. If the demerger occurred before concluding the proceedings to ascertain the entity's responsibility, the judge must take account of the financial situation of the original entity and not that of the entity resulting from the demerger.

In the event of transfer or assignment of the business within the scope of which the crime was committed, subject to the prior discussion benefit of the transferor entity, the transferee is jointly and severally liable with the transferor entity for the payment of the pecuniary

penalty, up to the limit of the value of the transferred business and up to the limit of the pecuniary penalties stated in the obligatory accounting records or due because of unlawful acts about which the transferee was aware in any case.

2. RENANTIS SPA: THE COMPANY AND ITS INTERNAL CONTROL SYSTEM

The Company operates in the production of energy from renewable sources and in the sector of integrated environmental services; in particular, it produces energy from wind, sun, biomass and waste-to-energy. In addition, through its subsidiaries, it provides a management and maintenance service for its own and third-party systems, for the production of energy.

The Company has been listed on the Euronext STAR Milan since 25 February 2002 and was delisted on 18 May 2022

By decision of the extraordinary shareholders' meeting of 26 July 2022, the Company adopted the "single tier" system of administration and control as provided under articles 2409-sexiesdecies et seq. of the Civil Code.

As such, the Company's corporate governance system is currently structured as follows:

- Shareholders' Meeting: the shareholders' meeting represents all shareholders. Its resolutions, passed in compliance with the law and articles of association, are binding for all shareholders. The shareholders' meeting has the authority to resolve, in ordinary and extraordinary sessions, on the matters reserved thereto by the law or by the articles of association. The Company currently has a sole shareholder Green BidCo S.p.A.
- Board of Directors: the Board of Directors is vested with full powers for the ordinary and extraordinary management of the Company without exceptions of any kind and has the power to undertake all acts that it considers appropriate to achieve the corporate purpose, only excluding those reserved for the Shareholders' Meeting by the law or by the articles of association;
- Chief Executive Officer: the Board of Directors, in accordance with Article 2381 of the Italian Civil Code, appointed a Chief Executive Officer, granting him/her extensive powers for the organisation and ordinary and extraordinary management of the Company, with the exception of matters that remain within the exclusive competence of the Board of Directors.

- Management Control Committee: the Management Control Committee comprises three members of the Board of Directors that it appoints, and is in charge of:
 - monitoring the adequacy of the organisational structure of the Company, the internal control system and the administrative and accounting system, and its suitability to properly report the company affairs;
 - carrying out any other tasks entrusted to it by the Board of Directors with special regard to relations with the party engaged to audit the accounts.
- Auditing Firm: the role of auditing and monitoring the Company's accounts is entrusted to a first-rate auditing firm.

3. THE MODEL

3.1 Structure of this document

This document is comprised of a “General Part” and a “Special Part”.

The General Part has the purpose of describing the provisions contained in the Decree, indicating the legislation specifically applicable to the Company, as to the relevant parts for the purposes of the Decree, describing relevant crimes for the Company, stating the exposed individuals, the principles regarding composition, appointment and operation of the Supervisory Body, indicating the system of penalties specific to breaches of the Model, stating the obligations concerning communication of the Model and the training of company staff.

The Special Part has the purpose of indicating the Sensitive Activity, that is, activities that have been considered by the Company as at risk of crime following risk assessments conducted pursuant to the Decree, general rules of conduct, information on prevention concerning said activities and essential control measures for the prevention and mitigation of unlawful acts.

In addition, the following are an integral part of the Model:

- the risk assessment aimed at identifying the Company's Sensitive Activity;
- Code of Ethics, which sets out the Company’s principles and rules of conduct;
- the Mechanisms for implementing the Model.

These documents are available in accordance with the procedures laid down for their dissemination within the company.

3.2 Purposes of the Model

With the adoption of the Model, the Company intends to comply strictly with the Decree and to improve and make as efficient as possible the existing internal control system and corporate governance.

The main objective of the Model is to create an organic and structured system of control principles and procedures, capable of preventing, as possible and actually feasible, the

commission of crimes set forth in the Decree. The Model will form the basis of the Company's governance system and will implement the process of disseminating a business culture based on fairness, transparency and legality.

In addition, the Model puts forward the following purposes:

- providing adequate information to Employees/Collaborators, as well as to those acting in the name, on behalf and in the interest of the Company, or who are connected to the Company itself by relevant contracts for the purposes of the Decree, with reference to activities involving the risk of the commission of crimes;
- disseminating a business culture based on lawfulness, inasmuch as the Company condemns any conduct not in accordance with the law and internal rules and, in particular, with the provisions contained in the Model itself;
- disseminating a control and risk management culture;
- implementing the effective and efficient organisation of business activities, emphasising in particular the making of decisions and their transparency and traceability, the accountability of resources dedicated to taking such decisions and respective implementation, the establishment of preventive and subsequent controls, as well as the management of internal and external information;
- implementing all measures necessary for reducing as much as possible and eliminating in the short term the risk of the commission of crimes.

3.3 Model and Code of Ethics

By Board of Directors resolution dated 21 July 2020, the Company updated its Code of Ethics, issued for all companies of the Group, the purpose of which is to inform the rules of conduct and ethical and social values by which the conduct of the Company and all exposed individuals targeted by the Model must abide. This applies in parallel with pursuit of the purpose and company objectives and consistently with that stated in this document.

The Model presumes compliance with the provisions of the Code of Ethics, forming therewith a body of internal rules aimed at disseminating a culture inspired by ethics and corporate transparency.

The Company's Code of Ethics is understood to be fully referenced herein and constitutes an essential basis of the Model, the provisions of which supplement the provisions herein.

3.4. Model of the subsidiaries of Renantis S.p.A.

Through its organisational units, the Company communicates the Model and each subsequent edition to the Employees/Collaborators, Supervisory Body and Management Control Committee.

Each Italian company controlled by Renantis S.p.A., whether directly or indirectly (including through Group companies in foreign jurisdictions), strives to adopt its own Model, following a resolution by its Board of Directors, after having analysed and identified the activities at risk of crime and the measures appropriate for preventing them. All the Italian subsidiaries, according to the definition in the specific Model, abide by the principles and contents of this document, unless the specific peculiarities inherent to the nature, size, business type, structure of internal delegations and powers do not match up with the implementation of different organisation principles and rules. It is the responsibility of each individual Italian company to adopt a specific Model and appoint its own Supervisory Body.

In addition, the Company also requires companies with headquarters abroad and direct or indirect subsidiaries of Renantis S.p.A. to adopt, in the management of activities involving the risk of commission of crimes of the same nature as those set forth in the Decree, a document referred to as "Compliance Programme", referencing the rules of conduct specified in the general part and in the (general and specific) prevention procedures set forth in this Model, in compliance with the applicable laws of the respective countries to which belonging as well as in the countries in which subsidiaries operate.

Lastly, the management and Employees/Collaborators of a foreign Group company operating in the name and/or on behalf of an Italian company of the Group, must abide by the rules of

conduct and prevention procedures contained in the Model adopted by the Italian company, available on the company intranet, as well as by the Compliance Programme of the specific company. Conversely, the Management and Italian Employees/Collaborators operating in the name and/or on behalf of a foreign company of the Group must also abide by the Compliance Programme adopted by the foreign company, as well as by the rules of conduct and prevention procedures contained in the Model of the specific company.

The Compliance Programme adopted by subsidiaries is communicated to the Company's Supervisory Body, which, as per the Model, informs the Board of Directors about it in the report in accordance with section 5.6. Any subsequent change of a significant nature made to the Model or Compliance Programme of subsidiary companies is communicated by the supervisory bodies, or, if it has not been established, or by the managing bodies of the subsidiary companies to the Company's Supervisory Body.

4. THE ADOPTION OF THE MODEL

4.1 Methodology for implementing the Model

The Model was developed taking into account the actual activities of the Company, its organisational and corporate structure, as well as the nature and size of its organisation in existence on the date of approval and future evolutions thereof, as reasonably foreseeable currently. It is also understood that the Model shall be subject to updates as necessary, based on the future evolution of the Company and on the context in which it operates.

For the purposes of implementation of the Model, the Company proceeded with a preliminary analysis of the specific corporate context and, subsequently, with an analysis of the business areas featuring potential risk profiles, with respect to the commission of the crimes indicated by the Decree. In particular, the following was analysed: the Company's history, the legislative context of reference, the existing corporate governance system, the system of powers and delegations, contracts existing with third parties, operating context, formalised practices and procedures disseminated within the Company for undertaking transactions.

For the purposes of preparing this document, the Company proceeded:

- identified the processes, sub-processes or company activities within which the predicate offences indicated in the Decree may be committed;
- with a risk assessment on the commission of crimes and on the internal control system capable of detecting unlawful conduct;
- with the identification of adequate control procedures, whether already existing or to be implemented as part of operational procedures and company practices, necessary for the prevention or mitigation of the risk of commission of the crimes as per the Decree;
- with the analysis of its system of delegations and powers and of attributing responsibilities.

The Company adopted this version of the Model, which replaces the previous one, by way of the Board of Directors resolution dated 23 June 2021.

4.2 Changes and updates to the Model

Changes to the Model fall under the exclusive responsibility of the Board of Directors, following disclosure to the Supervisory Body.

The Model must always be timely amended or supplemented, by Board of Directors resolution, including at the request of the Supervisory Body, in the event:

- of supervening significant changes to the legislative framework, organisation or activities of the Company;
- of supervening breaches or avoidance of the provisions contained therein, thereby demonstrating its non-effectiveness for the purposes of crime prevention.

In any case, any events making it necessary to change or update the Model must be reported in writing by the Supervisory Body to the Board of Directors, in order that it may pass resolutions under its responsibility.

Necessary changes to the corporate procedures for the implementation of the Model are undertaken by the involved Corporate Units, with the coordination of HR & Organisation. The Supervisory Body is constantly informed about the update and implementation of new operational procedures of the Group or those specific to the Company and has the power to issue its opinion on the change proposals. In the event that changes of an exclusively formal nature are necessary, such as clarifications or explanations for the text, the Company's Chief Executive Officer may take action independently, thereby reporting in a timely manner to the Board of Directors and Supervisory Body and thereby subsequently sending the updated text to the Corporate Unit in charge for publication thereof on the intranet and website.

4.3 Crimes applicable to the Company

Considering the structure and activities of the Company, the following predicate offences have been identified as relevant:

- offences committed in relations with the Public Administration (arts. 24 and 25 of the Decree);
- computer crimes and unlawful data processing (article 24-bis of the Decree);

- organised crime offences (art. 24-ter of the Decree) and transnational offences (art. 10, Law 146/2006);
- crimes against industry and trade (article 25-bis.1 of the Decree);
- corporate offences, including corruption in the private sector and incitement to corruption in the private sector (art. 25-ter of the Decree);
- crimes against the individual (article 25-quinquies of the Decree);
- culpable homicide or grievous or very grievous harm committed in violation of the rules on protection of health and safety at work (art. 25-septies of the Decree);
- crime of receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-money laundering (art. 25-octies of the Decree);
- crime relating to copyright violation (article 25-novies of the Decree);
- incitement not to make statements or to make false statements in court (art. 25-decies of the Decree);
- environmental offences (art. 25-undecies of the Decree);
- employment of illegally staying third-country nationals and encouraging the illegal stay of foreigners in national territory (art. 25-duodecies of the Decree);
- tax crimes (art. 25-quinquiesdecies of the Decree);
- offences relating to non-cash payment instruments (art. 25-octies.1 of the Decree);
- crimes against cultural heritage (arts. 25-septiesdecies and 25-duodevicies of the Decree).

4.4 Exposed Individuals under the Model

The Company's Model applies:

- to Employees;
- to Top management;
- to Company Representatives, even if abroad for the fulfilment of activities;

(collectively the "Exposed Individuals").

Exposed individuals under the Model are required to comply precisely with the provisions contained therein and with the respective implementing procedures.

This document constitutes an internal regulation of the Company and is binding for it.

5. SUPERVISORY BODY

5.1 Function

In fulfilment of the provisions of the Decree – which in art. 6, letter b), establishes as a condition for granting release from administrative liability the assignment of the task of overseeing the operation and observance of the Model to a Company body possessing independent control powers – the Company has established an autonomous and independent Supervisory Body with responsibility concerning risks control as per the Decree, connected to the specific activities undertaken by the Company itself and to the respective legal aspects.

The SB has the task of constantly monitoring:

- the observance of the Model by the exposed individuals thereunder, as identified in the preceding section 4.4;
- the actual efficiency of the Model in preventing the commission of the offences referred to in the Decree;
- the implementation of the provisions of the Model as part of the carrying-out of the Company's activities;
- the updating of the Model, in the event that it is discovered that there is the need to adjust it due to supervening changes to the company structure and organisation, to the Company's activities and to the legislative framework of reference.

The Supervisory Body possesses specific operating rules, approving the contents thereof and submitting them to the Board of Directors. The checking methods are generally structured in consideration: (i) of the information received through the regular information flows prepared by the Company, (ii) the information acquired during the regular meetings with the company representatives regarding the operation / development of the processes and the business, (iii) the results of the audits carried out by the Internal Audit Department of the Company.

5.2 Requirements and composition of the Supervisory Body

The members of the Supervisory Body must be selected exclusively based on the following requirements:

- autonomy and independence: the autonomy and independence of the Supervisory Body are key elements for the effectiveness of control activities.

The concepts of autonomy and independence do not have an absolute significance but must be set out and couched within the operational framework in which they are to be applied. Since the Supervisory Body has the tasks of verifying compliance by applied procedures, in company operations, its position within the entity must be to guarantee its autonomy from any form of interference and from influence from any member of the entity and, in particular, from the senior management with regard to operations, above all considering that the role held also consists of overseeing the activities of Senior individuals. As such, the Supervisory Body is placed in the Company's organisational structure at the highest possible hierarchical position and, in fulfilling this role, only answers to the Board of Directors.

In addition, to guarantee further the autonomy of the Supervisory Body, the Board of Directors makes corporate resources available thereto, according to the number and responsibilities in proportion to the tasks assigned thereto and approves, in the context of preparing the company budget, an adequate endowment of financial resources, as proposed by the Supervisory Body, which it may have at its disposal for all needs for properly fulfilling its duties (for example, specialist consultations, business trips, etc.).

The autonomy and independence of the Supervisory Body must be determined based on the role performed and on the tasks assigned thereto, identifying from whom and from what they must be autonomous and independent in order to perform such tasks. Consequently, the members of the Supervisory Body must not hold decision-making, operational or management positions such as to compromise the autonomy and independence of the entire Supervisory Body. In any case, the autonomy and independence requirements mean that the Supervisory Body must not be in a personal conflict of interest, even if potential, with the Company.

- Expertise: the Supervisory Body must possess internally adequate professional and technical expertise for the role that it is called upon to fulfil. Therefore, it is necessary that subjects with adequate professional skills in economic and legal matters as well as in the analysis, control and management of corporate risks are present within the SB. In particular, the SB must have the specialist technical skills necessary to carry out control and consultancy activities.

In order to ensure expertise useful and necessary for the Supervisory Body's activities and to guarantee expertise, as already highlighted, the Supervisory Body is assigned a specific budget for spending at its disposal, allowing for acquiring outside of the entity, when necessary, expertise in addition to its own. In this way, also by making use of external professionals, the Supervisory Body may endow itself with skilled resources, for example, in legal matters, corporate organisation, accounting, internal controls, finance and workplace safety, etc.

- Continuity of action: the Supervisory Body undertakes in a continuing manner the actions necessary for oversight concerning the Model with sufficient commitment and with the necessary investigative powers.

Continuity of action must not be understood as "continual business", since such an interpretation would necessarily impose a SB exclusively within the entity, whereas such a circumstance would instead result in a decrease in the indispensable autonomy that must characterise the SB itself. Continuity of action means that Supervisory Body activities must not be limited just to periodical meetings, but be organised based on an activity plan and on constant monitoring and analysis of the entity's system of preventive controls.

In compliance with the above criteria, the SB is composed of three members, two of whom are not Company employees. The Chair of the Supervisor Body shall be chosen from among the two members who are not employed by the Company. The internal member of the Supervisory Body shall be chosen, preferably, from among the corporate departments in charge of the supervision of the Company, and in any case, may not come from Corporate

departments that carry out operating or management functions or that are in any case exposed to the offence risks on the basis of the risk assessment carried out.

5.3 Eligibility and integrity requirements

The following may not be appointed as members of the Supervisory Body:

- those falling under the situations set forth in article 2382, Civil Code;
- the spouse, relatives and in-laws within the fourth degree of kinship of the directors of the company, the directors, spouse, relatives and in-laws within the fourth degree of kinship of the directors of the companies controlled by it, of the companies that control it and of those subject to common control;
- those linked to the Company, to the subsidiaries of the Company, to parent companies thereof or to those subject to joint control based on employment (to be considered on account of the organisational position/role) or based on a continuing, remunerated consultancy or service contract or based on other contracts of a pecuniary nature not compromising the independence thereof;
- those who own, directly or indirectly, shareholdings of such a size as to allow them to exercise a dominant or significant influence over the Company, pursuant to Article 2359 of the Italian Civil Code;
- those who have had a public-sector contract with central or local governments in the three years prior to appointment as a member of the Supervisory Body or to the establishment of the consultancy/collaboration contract with said Body;
- those in any other situation of clear or potential conflict of interest;
- those who have received a conviction, even if not final, or a pre-trial judgement imposing a fine in lieu of custodial punishment, even if not made irrevocable, or a judgement imposing a penalty upon request, pursuant to art. 444, et. seq., Code of Criminal Procedure, even if with a suspended sentence, subject to the effects of rehabilitation:
 - for one of the crimes provided for under Royal Decree no. 267 of 16 March 1972

- (bankruptcy law);
- for one of the crimes provided for under title XI of Book V of the Civil Code (companies and consortia);
 - for one of the crimes provided for against the Public Administration, against public trust, heritage, against the public economy or for a tax crime;
 - for one of the crimes provided for under laws that govern banking, financial, real estate or insurance activities and the laws on stock markets and securities, of payment instruments; for one of the crimes provided for under laws that govern banking, financial, real estate or insurance activities and the laws on stock markets and securities, of payment instruments;
 - for offences committed with criminal intent not included above, for having received a conviction or plea bargain, even if not yet definitive, even if with a suspended conviction with conditions, subject to discharge from bankruptcy, for a period of not less than a year;
 - for having been subject to an order for committal for trial related to an offence provided for under Legislative Decree 231/01;
 - those who have be subjected to prevention measures ordered by the Courts pursuant to Legislative Decree no. 159 of 06/09/2011 “Code of anti-mafia laws and prevention measures, as well as provisions on anti-mafia documentation, pursuant to articles 1 and 2 of Law no. 136 of 13 August 2010”.

The application of even one condition means non-eligibility for a position as member of the Supervisory Body.

5.4 Appointment, removal, replacement, loss of office and resignation

After verifying satisfaction of the requirements as per the preceding sections, the Board of Directors appoints the Supervisory Body, basing its decision not just on curriculums, but also on official statements collected directly from the candidate(s). In addition, the Board of

Directors receives from each candidate a statement confirming the absence of reasons for non-eligibility as per the preceding section.

After the formal acceptance of the appointed subjects, the appointment is communicated to all levels of the company through internal communication.

The SB remains in office until the end of the term of office of the Board of Directors that appointed it. If a member of the Supervisory Body is identified as a party external to the Group, the former may be re-elected following a specific assessment by the Board of Directors.

The removal of a Supervisory Body member from the position may only occur for just cause and will be decided by a Board of Directors resolution for one of the following reasons:

- failure to remain in compliance with the requirements as per the preceding sections;
- failure to remain in compliance with the requirements as per the preceding sections;
- breach of confidentiality duties;
- “failure or insufficient supervision” by the Supervisory Body – in accordance with the provisions of article 6, paragraph 1, letter d) of the Decree – serious and ascertained reasons of incompatibility that negate the independence and autonomy;
- Unjustified absence in two or more consecutive meetings of the Supervisory Body, after they have been properly called;
- the attribution of operating functions and responsibilities within the corporate organization that are incompatible with the requirements of “autonomy and independence” and “continuity of action” of the Supervisory Body;
- serious and ascertained reasons of incompatibility that nullify the independence and autonomy

The Supervisory Body is required to inform the Board of Directors, through the Chairman of the Supervisory Body itself, of the failure to remain in compliance with the requirements as per the preceding sections.

The Board of Directors removes the member of the SB who is no longer suitable and, after adequate justification, promptly replaces him/her.

Loss of the integrity requirements, inability to carry out the duties or the emergence of any reasons for disqualification constitute a reason for losing the position.

Additionally, with specific reference to the internal member of the Supervisory Body, the following shall constitute reasons for removal:

- the attribution of operating functions and responsibilities within the corporate organization that are incompatible with the requirements of “autonomy and independence” and “continuity of action” of the Supervisory Body;
- serious and ascertained reasons of incompatibility that nullify the independence and autonomy.

Each member of the SB may resign from office at any time by means of a written communication to be handed over to the Chairman of the Board of Directors.

In the event of termination or resignation of one of the members of the SB, the Board of Directors promptly replaces the member who has become unsuitable.

5.5 Remuneration of the Supervisory Body

The activities of the Supervisory Body shall be subject to the remuneration established upon appointment or by subsequent decision of the Board of Directors.

5.6 Functions and powers

The Supervisory Body meets at least four times a year and each time one of the members requests its convocation to the Chairman, justifying the appropriateness of the convocation. In addition, it may delegate specific functions to the Chairman. Minutes are taken of each Supervisory Body meeting.

For the fulfilment of the assigned duties, the Supervisory Body is vested with full powers to act and monitor all activities of the company and staff levels. It reports exclusively to the Board of Directors, to which it communicates through its Chairman.

The tasks and powers of the Supervisory Body and of its members may not be verified by any body or Corporate Unit, notwithstanding that the Board of Directors may verify consistency

between the activities actually undertaken by the Supervisory Body and the powers assigned thereto. In addition, subject to prevailing legal provisions, the Supervisory Body has free access – without the need for any prior consent – to obtain any information or data considered necessary for fulfilling its duties.

The Supervisory Body fulfils its duties by coordinating with other Corporate Bodies or Corporate Units at the Company. In particular, the Supervisory Body coordinates with the Corporate Units in charge of the Sensitive Activity as to all aspects concerning the implementation of operating procedures for implementation of the Model and, for undertaking its activities, may make use of Internal Audit Staff. In addition, the Supervisory Body may make use of the assistance and support of Corporate Units and of external consultants, in particular for problems requiring assistance in the form of specialist skills.

The Supervisory Body organises its activities based on an annual plan of action, by way of which it plans the actions to be taken for evaluating the effectiveness and efficacy of the Model, as well as the updating thereof. This plan is communicated to the Board of Directors. The Supervisory Body determines its annual budget and submits it to the approval of the Board of Directors. The Supervisory Body may not have to stay within the budget assigned, i.e. if the budget is insufficient to carry out the necessary tasks. In these cases, the Supervisory Body will notify the Chairman of the Board of Directors and report to the next meeting of the Board of Directors on why it could not stay within the budget.

In overseeing the actual implementation of the Model, the Supervisory Body possesses powers and duties that it exercises to ensure compliance with the laws and individual rights of workers and interested parties.

In particular, the SB:

- undertake or arrange for the undertaking of periodical inspections, under its direct surveillance and responsibility;
- access all information regarding the Company's Sensitive Activity;
- request information or the presentation of documents concerning Sensitive Activity to all Corporate Units involved and, if necessary, to Corporate Bodies and to parties

appointed in compliance with the provisions of accident prevention and workplace health and safety protection legislation, without prior authorisation and without giving any notice;

- request information or the presentation of documents regarding Sensitive Activity to the Exposed Individuals under the Model without prior authorisation and without any notification;
- carry out checks and inspections, including unscheduled ones;
- assess the reports of possible breaches and/or failures to comply with the Model;
- check to ensure that the breaches of the Model were actually and adequately sanctioned in accordance with the penalty system adopted by the Company;
- verify the main corporate documents and contracts entered into by the Company with respect to Sensitive Activity and to compliance by the same with the provisions of the Model;
- propose to the holder of disciplinary authority the adoption of the necessary penalties;
- verify periodically the effectiveness, efficacy and updating of the Model and, if necessary, propose to the Board of Directors any changes and updates;
- assist the Company's Chief Executive Officer and the HR & Organization, Legal & Corporate Affairs and Communication & Stakeholder Engagement in specifying the training/disclosure plans for the Exposed Individuals under the Model in the context of the matters referred to in the Decree;
- can check the implementation of the training plans;
- can draw up, at least every six months, a written report to the Board of Directors, with the minimum contents indicated in paragraph 5.6 below;
- in the case of the occurrence of serious, urgent events, observed in the performance of its activities, inform the Board of Directors.

5.7 Supervisory Body information flows to the company bodies

The Supervisory Body has the obligation to report to the Board of Directors, by way of two procedures:

- on a continual basis, due to specific needs, including of an urgent nature;
- every six months, by way of a written report featuring the following information:
 - summary of the activities, controls carried out by the SB during the period and their results;
 - any discrepancies between procedures for implementing the Model and the Model itself;
 - any new scopes of commission of the crimes set forth in the Decree;
 - reports received from external or internal parties regarding any breaches of the Model and results of checks regarding said reports;
 - disciplinary procedures activated on the proposal of the SB and any penalties applied;
 - general assessment of the Model and its effective operation, with any proposals for additions and improvements in form and content;
 - any changes in the legislative framework of reference;
 - adoption or significant amendments to the Compliance Program;
 - reporting on the expenses incurred;
 - mass planning of supervisory activities for the following half-year period.

The Board of Directors, the Chairman and the Managing Director have the right to call a meeting of the SB at any time. Moreover, the Supervisory Body has, in turn, the power to request, through respective parties, the convocation of the Board of Directors, the Chairman or the Chief Executive Officer as above for urgent reasons. The meetings with the bodies to which the SB refers must be put on record and a copy of the minutes must be kept by the SB and by the bodies involved from time to time.

The SB also reports to the Management Control Committee, at least annually, on the application of the Model, its operation, updating and the relevant facts or events found. In particular, the SB:

- reports to the Management Control Committee about any deficiency discovered with respect to the organisational structure and to the effectiveness and operation of the procedures;
- reports on breaches of the Model by Company Representatives;
- reports on acts undertaken by such parties that may constitute crimes.

5.8 Information flows to the Supervisory Body

Periodic information flows

The Supervisory Body shall define a periodic information flow that is capable of monitoring the sensitive areas identified in the special part of this Model, through which to assess the exposure to the potential risk of committing the predicate offences that apply to the Company.

The information flows shall comprise information, data, statistics, schedules, news and documents that the company departments have to periodically prepare and send to the Supervisory Body.

The structure of the periodic information flows is communicated by the Supervisory Body to the applicable company departments, for the sections that pertain to them, and in relation to the inter-company contracts in effect.

Occasional information flows

In addition to the periodic information flows described above, all the information regarding the following must be promptly sent to the Supervisory Body by the applicable or interested Company Departments:

- orders and/or information from Criminal Police bodies or any other authority, subject to the secrecy obligations required under the law, revealing the course of investigations, including with respect to unknown persons, for any offences for which Legislative Decree 231/2001 applies, if those investigations involve the Company or in any case the Recipients of the Model;

- orders and/or information concerning the existence of significant administrative or civil proceedings or disputes, subject in any case to the secrecy obligations required by law, revealing the course of investigations, including with respect to unknown persons, relating to requests or actions by independent, financial administration, local administration Authorities, to the contracts with the Public Administration, the requests and/or the administration of public financing;
- requests for legal assistance forwarded to the Company by the staff in the case of criminal or civil proceedings against them for the Offences governed by the Decree;
- information relating to breaches of the Model with evidence of the penalties given or the orders to file the proceedings with the related reasons;
- serious accidents (any accident with a recovery period of more than 40 days) which occur to employees or business partners of the Company and all those who have access to the Company's departments;
- environmental accidents that occur at the Company's offices or plants;
- any reports from *Internal Audit* Staff revealing anomalies or critical issues with respect to the Sensitive Activity identified in this Model.

Also, by determining a specific operating procedure and/or by supplementing existing procedures, the Supervisory Body may establish further types of information that supervisors involved in the management of Sensitive Activity must send, indicating the frequency and procedures by which said communications are submitted to the Supervisory Body itself.

Reports

The Exposed Individuals under the Model must communicate directly with the Supervisory Body to report on any breaches to the Model, by way of the restricted internal mail or through the dedicated e-mail address odv-renantis@renantis.com.

Reports must describe in a detailed manner the events and persons subject to the reporting itself.

In addition, the Company makes available to Company Representatives, as well as to Third Parties and more in general to everyone with relations with it, the Whistleblowing Portal, by way of which it is possible to make allegations, including anonymously. Said portal can be accessed through both the Intranet site and the internet site www.renantis.com of the Renantis Group.

The Company is committed to adopting measures capable of ensuring confidentiality regarding the identity of the party sending information to the Supervisory Body. Actions solely intended to slow down the work of the Supervisory Body must be penalised.

The Supervisory Body undertakes however to protect the whistle-blowers from any form of retaliation, discrimination or penalties, and, in any case, the whistle-blower shall be assured that their identity will be kept confidential, subject to legal obligations and the protection of the rights of the Company or persons erroneously accused or those who act in bad faith.

The reports received and the documentation managed by the Supervisory Body in general shall be kept by the Supervisory Body in a paper-based or electronic file, for a period of ten years. Access to that file is permitted to members of the Board of Directors and any parties authorised as the occasion arises by the Supervisory Body.

6. PROVISION BY THIRD PARTIES

The provision of goods and services by Third Parties, which may concern Sensitive Activity, must be governed by a written contract.

Insomuch as possible, the contract must feature the following clauses:

- the commitment of the Third Parties to comply with, during the term of the contract, the Code of Ethics, Model and, in general, the provisions of the Decree and to operate in line with them;
- the power of Company to proceed with the rescission of the contract and with a consequential action for damages, if a violation of the Code of Ethics and of the Model, if applicable, is observed.

7. INTERCOMPANY SERVICE CONTRACTS

In addition to that specified in section 3.4, some of the “Sensitive Activity” identified in the “Special Part” section below may be undertaken by Corporate Units belonging to other Group Companies, even if foreign, based on intercompany service contracts. In the performance of these contracts, the Company providing the service must:

- comply with the ethical and behavioural principles defined uniformly at Group level and adopted by each Group Company with the adoption of the Code of Ethics;
- in accordance with the provisions of the Code of Ethics, apply an internal control system protecting from the possible commission of unlawful acts set forth in the Decree.
- undertake to comply with the Model (with special reference to the principles of behaviour and control that apply with respect to Sensitive Activity carried out on behalf of the Company).

8. DISCIPLINARY SYSTEM

8.1 General principles

Art. 6, paragraph 2, letter e) and art. 7, paragraph 4, letter b) of the Decree state, as a condition for the effective implementation of the Model, the introduction of a suitable system for penalising failure to comply with the measures stated in the model itself.

Therefore, the establishment of an adequate disciplinary system with penalties proportionate to the seriousness of the violation with respect to infringements of the rules referred to in this Model by Exposed Individuals constitutes an essential requirement for the effectiveness of the Model itself.

The established penalties shall be applied to every violation of the provisions contained in the Model and Code of Ethics regardless of the progression and outcome of any criminal proceedings initiated by the Courts, in the event that the conduct to be reprimanded meets the elements of a relevant crime pursuant to Legislative Decree 231/2001.

Furthermore, violations by an exposed individual of measures to protect whistle-blowers established by the Company and whistleblowing carried out with wilful malice or gross negligence that is proven to be unfounded may be penalised.

In any case, penalisation shall apply regardless of the commission of a crime and shall constitute a reaction by the Company to the failure to comply with procedures or rules of conduct referred to in the Model.

By way of example, the following actions constitute disciplinary breaches:

- the violation, including through omissions and any collusion with others, of the principles of the Model, implementing procedures thereof, Code of Ethics or other instruments established for their implementation;
- the drafting of untruthful documents, possibly through collusion with others;
- the facilitation, through omissive conduct, of the drafting by others of untruthful documents;
- the removal, destruction or alteration of documentation concerning the procedure to evade the system of controls established by the Model;

- hampering the supervisory activity of the SB;
- preventing access to the information and documents required by subjects responsible for monitoring procedures and decisions;
- engaging in any other conduct to evade the control system established by the Model;
- whistleblowing that is revealed to be unfounded, including anonymously, with wilful malice or with gross negligence.

8.2 Penalties against Employees/ Collaborators with an employment contract

The Model constitutes a set of provisions by which staff must abide, regarding rules of conduct and penalties: as such, any breach thereof means the imposition of a disciplinary procedure and respective penalties. All Employees are required to comply with the provisions contained in the Model.

The disciplinary system is applied against Employees/Collaborators with an employment contract in accordance with art. 7 of Law no. 300 of 20 May 1970 (so-called Workers' Statute) and current National Collective Labour Agreements for the category. If the fact also constitutes a breach of duties arising under the law or employment contract, such as to prevent continuance of the employment contract even temporarily, termination without notice may be decided upon, following a disciplinary procedure, pursuant to art. 2119, Civil Code.

More specifically, for Employees/Business Partners with employment relationships, the following penalties shall apply:

- Verbal warning: in the case of a slight failure to comply with the principles and procedures set out under the Model and the Code of Ethics due to the employee's negligence (for example failure to adopt prudent measures when filing the support documentation needed to reconstruct the operations of the Company in the 231 areas of risk, a delay in reporting the information due under the Model to the Supervisory Body, etc.;

- Fine: in the case of a failure to comply with the principles and rules of behaviour provided for under this Model and the Code of Ethics for non-compliant behaviour or inadequate behaviour to the extent of being considered as having a certain severity (for example breach by someone of the obligations to inform the Supervisory Body of irregularities committed in the performance of their activities; repeated failure to take part, without a justified reason, in the training sessions given by the Company with respect to Legislative Decree 231/2001, the Organisation, management and control Model, or the Code of Ethics or Code of Conduct or regarding the related matters, etc.);
- Suspension of service and remuneration: in the case of serious procedural breaches to the extent of exposing the Company to liability with respect to third parties (for example: the failure to comply with the provisions of the Code of Ethics; the failure to issue or issue of false declarations with respect to compliance with the Model; the failure to comply with signatory power provisions and the delegation of authority system; the failure to supervise the behaviour of staff operating under their area of responsibility in order to ensure their actions in sensitive areas; breach of the obligations to provide the Supervisory Body with information on every situation or risk of the occurrence of the predicate offences found in the performance of their activities. In addition, with regard to whistle-blowing, this penalty, if an employee, within the scope of their work, and with malice, reports an unlawful action with respect to another party which is later found out to be false or without grounds, or if an employee breaches the measures aimed at protecting the whistle-blower);
- Dismissal, if an employee, when carrying out their activities, behaves in a way that does not comply with the provisions of the Model and the Code of Conduct, unequivocally aimed at carrying out an offence sanctioned by the Decree and which could determine the application of administrative penalties resulting from the offence provided under the Decree against the Company (for example in the case of repeated failure to comply with the provisions of the Model and the Code of Ethics;

intentional failure to carry out the requirements provided under the Model or the Code of Ethics; adoption, in the 231 areas of risk, of behaviour that does not comply with the provisions of the Model unequivocally aimed at carrying out one of the offences provided for under the Decree; failure to provide the Supervisory Body with relevant information relating to the commission, including attempted, of one of the predicate offences);

- Dismissal without notice for just cause in the case of a breach that is so serious (due to the wilful misconduct of the fact, or the criminal or monetary consequences or if it is a repeated offence) that it does not permit the continuation, including temporary, of employment (for example fraudulent behaviour unequivocally aimed at committing one of the offences provided under the Decree to the extent of destroying the trust relationship with the employer; drawing up incomplete or untrue documentation wilfully aimed at preventing transparency and checking the actions carried out; wilful breach of the procedures with external relevance; failure to draw up the documentation provided under the Model; breach or wilful avoidance of the control system provided by the Model regardless of how carried out, including the removal, destruction or alteration of the documentation relating to the procedure; behaving in a way that obstructs or avoids the inspections of the Supervisory Body, preventing access to the information and documentation by the parties in charge of the inspections or the decisions).

For Employees/Business Partners classified as "manager", the following shall apply:

- Written warning and requirement to comply with the provisions of the Model in the case of the non-serious breach of one or more of the rules of conduct or procedural rules provided under the Model and in the Code of Ethics;
- The suspension, as a precautionary measure, of the work services in the case of serious breach of one or more rules of conduct or procedural rules provided under the Model and the Code of Ethics;
- Dismissal for just cause in the case of repeated and serious breaches of one or more

provisions of the Model and the Code of Ethics to the extent of irreparably destroying the relationship of trust, not permitting continuation, including temporary, of the employment relationship (for example in the case in which a manager repeatedly breaches the measures provided for the protection of whistle-blowers within the scope of a working relationship or makes repeated malicious reports against another party within the scope of the work relationship which turn out to be false or groundless).

8.3 Measures against Directors

If the breach concerns a director of the Company, the Supervisory Body must immediately provide notice thereof to the Board of Directors through a written report. In this case, the Board of Directors may impose any measure established under law, to be determined based on seriousness, fault and harm resulting from the Company. More specifically, Directors who do the following shall be laid off from the position or have the delegations of authority withdrawn (with the consequent reduction of the remuneration):

- behave in a way that does not comply with the Model and/or with the Code of Ethics, carrying out actions that cause or could cause damage to the company, exposing it to an objective situation of danger with regard to the extent of the assets;
- behave, in the performance of the activities at 231 risk, in a way that does not comply with the provisions and the procedures referred to in the Model and/or in the Code of Ethics and is unequivocally aimed at carrying out an offence sanctioned under Legislative Decree 231/2001.

In more serious cases and when the breach is such that it harms the fiduciary relationship with the Company, the Board of Directors proposes removal from the position in a Shareholders' Meeting.

8.4 Measures against members of the Supervisory Body

For measures against members of the Supervisory Body, refer to the provisions on removal from their position under section 5.4.

The Board of Directors adopts protective measures to avoid retaliation or actions discriminating against or harmful to members thereof. In particular, the adoption of disciplinary penalties as well as any act modifying or discontinuing the Company's relationship with certain members of the Supervisory Body is subject to the prior, justified approval of the Board of Directors.

Measures against Third Parties

Relations with Third Parties are governed by suitable formal contracts, which must establish clauses on compliance with the Decree and the fundamental principles of the Code of Ethics by certain parties. In particular, non-compliance by them must lead to the termination of such relations, subject to a claim for damages if the conditions are met.

9. COMMUNICATION AND TRAINING OF COMPANY PERSONNEL

External communication of the Model and of its fundamental principles is overseen by Communication & Stakeholder Engagement who ensures their dissemination and disclosure to the Recipients, as well as to the community in general, through the means considered most appropriate (for example, company website, specific brochures, etc.).

With the support of the HR & Organization, Legal & Corporate Affairs Units and the involvement of the Supervisory Body, it is the Company's responsibility to implement and formalise specific training plans, with the aim of ensuring actual knowledge of the Decree, Code of Ethics and Model by all Exposed Individuals (for whom this information is mandatory).

The provision of training must be different depending on whether it relates to exposed individuals in general, to exposed individuals operating in specific areas of risk or to Directors, etc., based on the analysis of expertise and training needs undertaken.

The Supervisory Body oversees the actual implementation of training plans.

The Company guarantees means and methods that always ensure the traceability of training initiatives and the formalisation of the attendance of participants, the possibility of evaluating their level of learning and the evaluation of their level of satisfaction with the course in order to develop new training initiatives and improve those currently underway, also through comments and suggestions on content, material, teachers, etc.

Training, which may also be provided remotely or through the use of electronic systems, the contents of which are examined by the Supervisory Body, is undertaken by experts in the subjects set forth in the Decree.

SPECIAL PART

1. INTRODUCTION

Pursuant to what is established by Article 6, paragraph 1, let. a) of the Decree, the Company, through a process of mapping activities and assessing existing risks and controls as part of the company context (risk assessment), identified the Sensitive Activity (divided by type of offence and listed in the following paragraphs), within which offences among those covered by the Decree can potentially be committed.

In order to prevent or mitigate the risk of committing such crimes, the Company has consequently put forward general rules of conduct and general protocols for prevention, applicable to all Sensitive Activity, and specific protocols for prevention, for each of the identified at-risk activities.

2. GENERAL RULES OF CONDUCT

Exposed Individuals under the Model abide by rules of conduct in accordance with the law, the provisions contained in this document, the principles contained in the Code of Ethics and in instruments implementing the Model, in order to prevent the occurrence of crimes established by the Decree.

In particular, the principles identified in the Code of Ethics, which are understood to be fully referenced herein, relating to the various types of Exposed Individuals, constitute a premise and integral part of the protocols for prevention as per section 3 below.

For the purposes of adopting and implementing the Model, the protocols indicated below also apply.

3. GENERAL PREVENTION PROTOCOLS

The following general prevention protocols are implemented for all operations concerning Sensitive Activity, as described in the following Sections:

- only subjects who have been previously identified through delegation of powers, proxies, organisational charts, job descriptions, procedures, organisational provisions/written warnings of reprimand are entitled to carry out Sensitive Activity;
- only subjects that have been previously identified for this purpose are qualified to deal with all third-party counterparties;
- the system of external delegations and powers of signature is consistent with the responsibilities assigned to each subject and the knowledge of these powers by external subjects is guaranteed by proper means of communication and advertising;
- the formation and implementation of decisions of the Company comply with the principles and requirements contained in law provisions, in the articles of association, in the Code of Ethics and in the Model implementation instruments;
- the management, coordination and control responsibilities within the Company are formalised;
- the levels of hierarchical structure are formalised and the different tasks in the Company are described;
- training phases and authorisation levels of the deeds of the Company are always documented and traceable;
- the allocation and exercise of powers in a decision-making process are consistent with positions of responsibility and with the relevance and/or critical aspects of the underlying economic transactions;
- there is no subjective identity between those who take or carry out the decisions, those who are required to control them as envisaged by law and by the procedures contemplated by the internal control system;
- for all operations at risk concerning Sensitive Activity, guidelines are implemented and carried out by the Manager of the Corporate Unit responsible for managing the considered operation at risk. The Unit Manager:
 - can ask for information and clarification to all the Corporate Units or individual subjects dealing with or that have dealt with the operation at risk;

- promptly informs the SB of any critical issues;
- must consult the SB in all cases of inefficiency, inadequacy or problems when carrying out the prevention protocols or operating procedures for implementing them or in order to obtain clarifications regarding the objectives and methods of prevention envisaged by the Model;
- access to Company data is in compliance with the European General Data Protection Regulation 2016/679 (“Data Protection Regulation”), Legislative Decree 196/2003, as subsequently amended and modified, (“Data Protection Code”), as well as any other applicable regulation regarding the processing of personal data;
- documents relating to the formation of decisions and their implementation are filed and stored by the respective Corporate Unit. Accessing documents already filed is restricted only to persons authorised according to the Group's operating procedures, as well as to the Management Control Committee, to the auditing company and to the SB;
- the SB makes sure that the operating procedures regulating Sensitive Activity, which are an integral part of the Model, fully implement the principles and provisions contained in this Special Part, and that they are constantly updated, also on proposal of the SB, in order to ensure the achievement of the purposes of this document.

4. INTERCOMPANY SERVICE CONTRACTS

As already mentioned in the General Part, some of the Sensitive Activity identified in the following sections may be carried out by Corporate Units belonging to other Group Companies, including foreign ones, and/or by the same Company for subsidiaries, on the basis of intercompany service contracts, in accordance with the ethical and conduct-related principles set forth in the Group Code of Ethics and in this Model (as to the applicable parts).

A. OFFENCES COMMITTED IN RELATIONS WITH THE PUBLIC ADMINISTRATION (ARTICLES 24 AND 25 OF THE DECREE)

A.1 Introduction

The concept of Public Administration in criminal law is understood in a broad sense, encompassing the entire activity of the State and other public entities; therefore, offences against the Public Administration pursue facts that prevent or disturb the regular carrying-out not only of the administrative - in technical terms - but also legislative and judicial activities. Therefore, the Public Administration is understood as the set of all public functions of the State or other public entities.

The subjects representing the Public Administration for the purposes of criminal law are those who perform a public function or a public service.

Public function means activities regulated by public law concerning the legislative (States, Regions, Provinces with special powers, etc.), administrative (state and local governments, Police, supranational administrations, Authority, Chambers of Commerce, housing committees, inspectors of public works, experts of the Italian Shipping Register, etc.), judicial (courts, process servers, auxiliary bodies of the Administration of Justice such as assignees in bankruptcy, etc.) functions.

The public service is characterised by exercising the:

- authoritative power, namely the power that allows the Public Administration to achieve its purposes through actual commands, with regard to which the recipient is in a position of subjection. This is the activity in which the public-law power - which includes both the power of coercion (arrest, search, etc.) and law-breaking contestation (establishment of fines, etc.), as well as the powers of hierarchical supremacy within public offices - is expressed;
- certifying power, namely the power to establish a fact with probatory efficacy.

Public service means activities regulated by public law, characterised by the lack of authoritative or certifying powers typical of the public service, with the exclusion of the carrying-out of simple clerical tasks and the provision of merely material work.

Subjects carrying out a public service are called public officers or public servants.

The public officer can form or express the will of the Public Administration or exercise authoritative or certifying powers.

By way of example but not by way of limitation, members of state and local governments, members of supranational administrations (e.g. of the European Union), NAS, NOE, members of the Supervisory Authorities, members of the Police and Guardia di Finanza, members of the Chambers of Commerce, directors of public economic entities, courts, process servers, auxiliary bodies of the Administration of Justice (e.g. assignees in bankruptcy) are considered Public Officers.

On the other hand, the Public Service Appointee carries out activities relating to the care of public interests or the satisfaction of needs of general interest submitted to the supervision of a public entity. The criminal law clarified that the bureaucratic classification of the subject in the structure of a public entity is not a criterion for recognising the Public Service Appointee, because what matters is the activity actually carried out by the subject. Therefore, a private individual or an employee of a private company can also be qualified as a Public Service Appointee when carrying out activities with a view to pursuing a public purpose and the protection of public interest.

By way of example but not by way of limitation, the employees of the national health service, the cash office staff of a public entity, the employees of hospitals, local health centres, Italian workers' compensation authority, Italian social security organisation, employees of the municipal energy companies, post offices, customs offices, members of town councils, employees of companies operating public services (for example, railways, motorways, etc.) ENI (National Hydrocarbon Corporation) and those carrying out waste disposal activities can be considered as Public Service Appointees.

A.2 Applicable offences

Based on the analyses carried out, the following offences committed in relations with the public administration are considered as applicable to the Company:

- **embezzlement of public funds**, envisaged by Article 316-bis of the Italian Criminal Code and identifiable whenever anyone, outside the Public Administration, has been granted from the State or other public entity or from the European Communities contributions, subsidies, loans, subsidised loans or other funds of the same type, regardless of what they are called, to be used for the realisation of one or more purposes, does not use them for the specified purpose, shall be punished with imprisonment from six months to four years;
- **misappropriation of public funds**, envisaged by Article 316-ter of the Italian Criminal Code and identifiable whenever anyone, save that the fact constitutes an offence envisaged by Article 640-bis of the Italian Criminal Code, by using or submitting false declarations or documents, or declarations and documents containing false statements, or by omitting any information due, obtains unduly, for oneself or others, contributions, subsidies, loans, subsidised loans or other funds of the same type, however they are called, granted or issued by the State, other public authorities or the European Communities;
- **fraud against the State or another public entity**, envisaged by Article 640 of the Italian Criminal Code, paragraph 2, no. 1 and identifiable whenever anyone, with devices or tricks, misleading someone, obtains, for himself or someone else, an unlawful profit to the detriment of third parties, if the deed is committed to the detriment of the State or another public entity or with the excuse of having someone discharged from military service;
- **aggravated fraud for the purpose of obtaining public funds**, envisaged by Article 640-bis of the Italian Criminal Code and consisting in the same behaviour referred to in the paragraph above, if carried out to obtain contributions, subsidies, loans, subsidised loans or other funds of the same type, however they are called, granted or issued by the State, other public entities or the European Communities;
- **computer fraud against the State or other public entity**, envisaged by Article 640-ter of Italian Criminal Code and identifiable whenever anyone, by changing in any way the

operation of an IT or telematic system or by intervening in any way without any right on data, information or programmes contained in an IT or telematic system or pertaining to it, gets an unlawful profit for oneself or others to the detriment of the State or another public entity;

- **corruption with the intent to influence an official act** envisaged by Article 318 of the Italian Criminal Code and identifiable whenever the Public Officer who, in the exercise of his/her duties or powers, unduly receives, for himself/herself or a third party, money or other benefits or accepts the promise thereof;
- **bribery to achieve an act by a Public Officer in breach of official duties**, established by Article 319 of the Italian Criminal Code, identifiable whenever the Public Officer receives, for himself/herself or a third party, cash or other benefits, or accepts the promise thereof, to omit or delay, or due to having omitted or delayed, an official act, or to perform or due to having performed an act contrary to official duties;
- **judicial corruption**, envisaged by Article 319-ter of the Italian Criminal Code and consisting in actions of corruption, if committed to favour or damage a party in a civil, criminal or administrative case;
- **unlawful incitement to give or promise benefits**, envisaged by Article 319-quarter of the Italian Criminal Code and identifiable whenever the Public Officer or Public Service Appointee who, taking advantage of his/her capacity or of his/her powers,
- **induces someone to unlawfully give or promise money or other benefits to him/her or to a third party; corruption of a Public Service Appointee**, envisaged by Article 320 of Italian Criminal Code, identifiable whenever anyone as set forth in Articles 318 and 320 of the Italian Criminal Code envisages the application of the same provisions when the behaviour referred to therein is carried out by a Public Service Appointee.

Pursuant to Article 321 of the Italian Criminal Code (“punishments for the briber”), the punishments established by Articles 318, paragraph 1, 319, 319-bis, 319-ter and 320 of the Italian Criminal Code in relation to the cases of Articles 318 and 319 of Italian Criminal Code,

also apply to those who make or promise to give cash or other benefits to a Public Officer or Public Service Appointee;

- **unlawful trafficking of influences, established by art. 346-bis of the Italian Criminal Code, consisting of the conduct of a person who, by exploiting or claiming existing or alleged relations with a Public Officer or a person in charge of a public service or one of the other parties referred to in article 322-bis, unduly arranges the giving or promising, to himself or others, of money or other benefits, as consideration for own unlawful mediation with a Public Officer or a person in charge of a public service or one of the other parties referred to in article 322-bis, or to remunerate the same in relation to the exercise of respective duties or powers;**
- **incitement to corruption, envisaged by Article 322 of the Italian Criminal Code and identifiable whenever anyone offers or promises undue money or other benefits to a Public Officer or a Public Service Appointee for the exercise of their functions or powers or to incite them to omit or delay an official act should the offer or promise not be accepted;**
- **corruption and incitement to corruption of members of the boards of the European Communities and of officials of the European Communities and Foreign Countries, envisaged by Article 322-bis of the Italian Criminal Code, and under which the provisions referred to in Articles 314, 316, from 317 to 320 and 322, paragraphs 3 and 4, of the Italian Criminal Code also apply:**
 - to members of the Commission of the European Communities, of the European Parliament, of the Court of Justice and of the Court of Auditors of the European communities;
 - to officials and agents employed under the charter in accordance with the Staff Regulations of Officials of the European Communities or the Conditions of Employment of agents of the European Communities;

- to persons under the control of the Member States or of any public or private entity of the European Communities, who perform functions corresponding to those of the officers or agents of the European Communities;
- to members and people in charge of entities incorporated on the basis of the Treaties drawn up by the European Communities;
- to those who, within other Member States of the European Union, perform functions or activities corresponding to those of Public Officers and Public Service Appointees.

The provisions referred to in Article 321 and 322, paragraphs 1 and 2 of the Italian Criminal Code, apply even if money or other benefit is given, offered or promised:

- to the persons indicated in the first paragraph of Article 322-bis;
- to persons who perform functions or activities corresponding to those of Public Officers and Public Service Appointees within other foreign States or international public organisations, if the fact is committed to obtain for oneself or others an illegal benefit in international business transactions or to obtain or maintain a business or financial activity.

The persons indicated in the first paragraph of Article 322-bis are treated as Public Officers, if they perform corresponding functions, and as Public Service Appointees in other cases.

A.3 Sensitive Activity

The Company identified the Sensitive and instrumental activities that can be carried out in its own interest and/or in the interest of a subsidiary, also by virtue of specific intra-group contracts within which, potentially, some of the offences in relations with the Public Administration envisaged by Articles 24 and 25 of the Decree could be committed:

- public relations and institutional relations, participation in conferences and meetings organised by public entities (Municipalities, Provinces, Regions, etc.) and trade associations;
- assistance for subsidiaries in related business activities including, but not limited to:

- management of relations with the Public Administration, including, but not limited to, (i) requests for opinions, authorisations, licences or authorisations for the acquisition / development / construction / operation of energy production plants with renewable and non-renewable sources, (ii) inspections, (iii) energy efficiency improvement for buildings and public roads including “smart” energy management;
- activities to acquire/establish rights in areas owned by local/private bodies, to be allocated to the development/construction of energy production plants with renewable and non-renewable sources and expropriation procedures;
- management of subsidised loans or other government funding;
- treasury, payments and funds management, as well as Public Administration-related credit management;
- management of corporate affairs and extraordinary transactions;
- management of intercompany relations;
- management of disputes;
- personnel selection, recruitment and development;
- administrative management of personnel and reimbursement of expenses;
- management of capital goods and company benefits (e.g. cars, mobile phones, personal computers, corporate credit cards, etc.);
- management of gifts, gratuities, donations and sponsorship;
- management of purchases of goods and services;
- sales, marketing and business development management;
- provision and management of fiduciary advice (of a legal, technical, notarial and tax nature);

A.4 Specific prevention protocols

For transactions concerning public relations and institutional relations, participation in conferences and meetings organised by public entities (Municipalities, Provinces, Regions, etc.) and trade associations, the protocols establish that:

- the meeting must be reported by preparing the minutes/memo with the indication of the representative of the PA, the trade association or the supervisory and control authority met, the subject of the meeting, its results and any other relevant information;
- the document must be properly filed by the Corporate Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- I_STAFF12.GR "Operating instruction for the management of relations with the Public Administration";
- P_STAFF01.GR "Employee Group Handbook – HR Procedure";
- "Guidelines for the management of relations with the Public Administration¹".

For transactions concerning "**Assistance for subsidiaries in related business activities**", find below the activities and respective protocols.

With reference to the "**Management of relations with the Public Administration, including, but not limited to, requests for opinions, authorisations, licences or authorisations for the acquisition / development / construction / operation of energy production plants with renewable and non-renewable sources, (ii) inspections, (iii) energy efficiency improvement**

¹The Guidelines for the management of relations with the Public Administration forms an integral part of the OMM, as with the specific prevention protocols.

for buildings and public roads including “smart” energy management, the protocols provide that:

- transparency, traceability and verifiability of the relations with the Public Administration are guaranteed, in accordance with the rules and operating procedures provided for by the applicable reference procedures;
- all documents, requests and formal communications, which are intended for the Public Administration, must be managed and signed only by the respective Corporate Units and signed only by persons previously identified and authorised by the Company;
- the Unit Manager for the implementation of the operation must authorise in advance the use of data and information concerning the Company and intended for documents, notices, certificates and requests of any kind to be sent to the Public Administration in general;
- the Unit Manager for the implementation of the operation must make sure that the documents, declarations and information sent by the Company to obtain the granting of concessions, permits, certifications, licences and authorisations are complete and truthful;
- relations with government counterparties at meetings, conferences or exchanges of letters, in particular when decisions need to be taken, to accept or object to government decisions, or in any other way to bind the Company, must be overseen by formally delegated corporate parties, in accordance with the organisational structure and the tasks performed;
- at institutional/formal meetings with officials of the Public Administration or Supervisory Authorities, as possible, at least two authorised company representatives/proxies must participate;
- the authorised persons must report the meetings held with representatives of the Public Administration and the key aspects arising during the meetings to the hierarchical and functional Manager;

- upon the sending of information to the Public Administration through software provided by it, as applicable, parties must comply with the safeguards set forth in paragraph B.3 of this Special Section, with reference to the Sensitive Activity of “Management of IT Systems”;
- the document must be properly filed in a specific archive by the Corporate Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- I_STAFF12.GR “Operating instruction for the management of relations with the Public Administration”;
- P_BUSLN01.GR Procedure for the management of Business Development and M&A activities”;
- P_BUSLN02.GR “Procedure for managing Engineering & Construction activities”;
- P_BUSLN05.GR “Procedure for defining and monitoring Business Asset Governance activities”;
- P_BUSLN06.GR “Procedure for managing Thermal Generation activities”;
- P_BUSLN08.GR “Procedure for managing Technical Asset Management activities”
- P_BUSLN03.GR “Procedure for managing Energy Management & Downstream Services activities”;
- P_STAFF04.GR “Procedure for managing Legal activities”;
- "Guidelines for the management of relations with the Public Administration".

With reference to “ Activities to acquire/establish rights in areas owned by local/private bodies, to be allocated to the development/construct ion of energy production plants with

renewable and non-renewable sources and expropriation procedures” the protocols establish that:

- information must be given on the procedure followed for identifying land and establishing rights in rem and rights to the use thereof (including a description of the purpose, amount and reasons underlying the choice), as well as for choosing any real estate broker;
- the establishment of rights in rem and rights to use land and any real estate brokerage contracts must always be governed by a written agreement, signed by parties with appropriate powers clearly establishing the price and the purpose of the service;
- specific checks must be carried out on the fairness of the price for the establishment of rights in rem and rights to use the land (in particular, consistency with market values);
- the produced, sent and received documentation must be properly filed in a specific archive by the Corporate Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”;
- P_BUSLN01.GR Procedure for the management of Business Development and M&A activities”;
- P_STAFF05.GR “Purchasing procedure”;
- P_STAFF08.GR “Administrative and accounting procedure for the management of the Purchase Cycle”;
- P_STAFF04.GR “Procedure for managing Legal activities”;
- "Guidelines for the management of relations with the Public Administration".

With reference to the **"Management of subsidised loans or other public loans"** , the protocols establish that:

- in the case of relations with the Public Administration relating to the management of subsidised loans or other government funding, the protocols set forth in this paragraph, relating to relations with the Public Administration, must also be applied;
- the Unit Manager for the implementation of the operation must make sure that the statements and documents submitted in order to obtain the loan or contribution are complete and truthful and represent, as applicable, the real economic and financial situation of the Company;
- the documentation for applying for a loan or government contribution must be signed by a party with the necessary powers;
- the financial resources obtained as public loan must be allocated exclusively to the initiatives and to the achievement of the purposes for which they were requested and obtained;
- the use of these resources must always be justified by the applicant, who certifies that they are consistent with the purposes for which the loan was requested and obtained;
- the regularisation of the expected periodic amounts (for example fund transfers to the project current accounts, principal/charge instalment payments) are carried out in accordance with the loan contracts received;
- the consistency between the use of loans or contributions and the purposes for which they are disbursed must be verified, also with the assistance of any service providers involved;
- the documents must be properly filed by the Corporate Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- I_STAFF12.GR “Operating instruction for the management of relations with the Public Administration”;
- P_STAFF06.GR “Management of Structured Finance and Loans Administration transactions”;
- P_STAFF19.GR “Administrative and accounting procedure for the management of financial accounting and treasury activities”;
- P_STAFF01.GR “Employee Group Handbook – HR Procedure”;
- "Guidelines for the management of relations with the Public Administration".

With reference to “ Treasury, payments and funds management, as well as Public Administration-related credit management”, the protocols establish that:

- limits must be established on the autonomous use of financial resources by fixing quantity thresholds consistent with the managerial skills and organisational responsibilities;
- the Board of Directors must establish and amend, if necessary, the joint signature procedure for certain types of operations or for operations that exceed a certain quantitative threshold. The SB will be informed of this change;
- there must be no subjective identity between those who commit the Company with regard to third parties and those who authorise or order the payment of sums due on the basis of the commitments undertaken; where this is not possible in relation to individual operations, the SB must be informed;
- operations involving the use of economic or financial resources must have an explicit cause, must be motivated by the requesting subject, even though the mere indication of the type of expenditure to which the operation belongs, and must be documented and recorded in compliance with the principles of professional and accounting correctness;

- incoming and outgoing cash flows must not be allowed, except for minimal expenses (petty cash) expressly authorised by the competent Corporate Units envisaged by the applicable company procedure;
- with reference to banking and financial transactions, the Company must use only financial and banking intermediaries subject to transparency and fairness regulations in compliance with the European Union regulations;
- payments to third parties must be made through banking circuits with means that guarantee that the beneficiary of the payment is actually the third party contracting with the Company;
- monitoring of counterparties in the payment phase must be implemented in order to identify any counterparties with current accounts with banks or their branches located in “non-cooperative countries”² and/or suppliers/consultants/collaborators requesting payment through trust companies and trusts;²
- depending on the nature of the service provided, quantitative limits must be established in advance on the payment of cash advances and the reimbursement of expenses incurred by Employees with an employment contract with the Company. The reimbursement of expenses incurred must be requested by filling in specific forms and only after the production of appropriate documents supporting the expenses incurred;
- the Company's receipts and payments, as well as cash flows, must always be traceable and documentable;
- the methods (e.g. verbal or written reminder) by which the procedure for collecting credits from the Public Administration is to be implemented must be established;
- it is necessary to identify the subjects authorised to agree on a possible return plan with the PA;

² For all updates regarding tax legislation and relations between Italy and other countries regarding the management and exchange of tax information, refer to the Revenue Agency website: <http://www.agenziaentrate.gov.it/wps/content/Nsilib/Nsi/Documentazione/Fiscalita+internazionale/>

- also with reference to the settlement agreements with the PA, there is no subjective identity between the subject who negotiates within the assigned limits and the subject who definitively approves the agreement by signing it;
- the traceability of the subjects involved and of the requests for information received by the PA with regard to the reminders for payment and negotiations for the signing of settlement agreements must be guaranteed;
- the identified Manager must inform the SB of the start of the procedure, the results of the various phases of the activity, the conclusion of the procedure as well as any critical issues that may arise in the course of the procedure;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF19.GR "Administrative and accounting procedure for the management of financial accounting and treasury activities";
- P_STAFF08.GR "Administrative and accounting procedure for the management of the Purchase Cycle";
- P_STAFF09.GR "Procedure for managing guarantees";
- P_STAFF06.GR "Management of Structured Finance and Loans Administration transactions";
- P_STAFF15.GR "Administrative and accounting procedure for the management of hedges against financial risks";
- I_STAFF10.IT "Cash Management"
- "Guidelines for the management of relations with the Public Administration".

With reference to the "**Management of corporate affairs and extraordinary transactions**", the protocols establish that:

Corporate affairs

- operations must be carried out with the assistance of the Legal & Corporate Affairs Unit, also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- all documents relating to items on the agenda of meetings of the Board of Directors and of Shareholders' Meeting must be communicated and made available with reasonable advance notice with respect to the date of the meeting;
- the minutes of meetings of the company bodies and corporate books that are obligatory in accordance with prevailing laws are duly updated and they are safeguarded and complete;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Extraordinary transactions

- acquisition and/or merger transactions are carried out in coordination with the Business Development and M&A Division, in compliance with the rules and operating procedures required by the relevant applicable procedures;
- a preliminary evaluation of the target company is carried out for each transaction, and if there is an interest in pursuing the investment, formal due diligence is carried out which also includes a check of the opposite parties;
- the investment and related documentation (both supporting and finalising documentation for the transaction) are checked by the applicable company units and approved by the parties with the applicable powers;
- specific controls are carried out where possible regarding the consistency of the price/value of the extraordinary transaction with respect to market prices;
- the documents relating to extraordinary transactions must be properly kept by the company Unit Manager involved, in an adequate archive, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF13.GR “Administrative and accounting procedure for managing corporate affairs”;
- P_BUSLN01.GR Procedure for the management of Business Development and M&A activities”;
- P_BUSLN03.GR “Procedure for managing Energy Management & Downstream Services activities”;
- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”.

With reference to the “**Management of intercompany relations**”, the protocols establish that:

- all intercompany transactions must be valid, justifiable and carried out in the interest of the Company, must be mirrored in actual economic/financial transactions and must be governed by contracts signed by parties with appropriate powers;
- intercompany contracts must specify the purpose of the transaction, the nature of the services, the term, the payment conditions, the transfer prices and the calculation methods, as well as any offsetting methods;
- the definition of the transfer prices complies with the criteria defined in the Group transfer pricing policy;
- controls on the intercompany invoices received are implemented and periodic reports of the services provided are requested from the opposing party;
- a specific clause must be included: (i) requiring an express declaration by the intercompany counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Company’s Model (as applicable) and in the Group’s Code of Ethics; (ii) stating the consequences in the event of a breach of that declared (including the termination of the contract);

- it must be established under contract that the Company receiving the intercompany service may access the information it needs for oversight purposes;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

In the management of relations with related parties, the provisions of the “Procedure for Transactions with Related Parties”, as published at www.renantis.com– Ethics and Governance, shall also be applied.

In the management of intercompany relations, the provisions of the document "Guidelines for the management of relations with the Public Administration" are applied.

With reference to the “**Management of disputes**”, the protocols establish that:

- Company transactions must be carried out with the assistance of the Legal & Corporate Affairs Unit or, for tax-related disputes, of the Tax Unit also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- the commencement of a dispute must be authorised by a party with the necessary powers;
- a Manager must always be identified, consistent with the subject matter of the dispute, with the necessary powers to represent the Company or to formally assign the case to any external lawyers;
- the conclusion of the dispute, both in court (e.g. evaluation on the appropriateness of proceeding with higher instances) and out of court, must be approved by a party with the necessary powers;
- the traceability of the subjects involved and of the requests for information received during the dispute must be guaranteed as well as the assessment process and internal authorisation of the documents handed over during the dispute;

- the document must be properly filed by the Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF04.GR “Procedure for managing legal activities”;
- P_STAFF12.GR “Administrative and accounting procedure for the management of court and out-of-court disputes”
- "Guidelines for the management of relations with the Public Administration".

With reference to transactions concerning **“Personnel selection, recruitment and development”**, protocols must establish that:

- activities relating to the selection and recruitment of personnel as well as subsequent career promotions must be conducted with the aim of ensuring that this process is carried out on the basis of effective corporate needs, in a transparent and documentable manner, based on non-arbitrary criteria, in compliance with impartiality, meritocracy and non-discrimination principles;
- for each request for personnel, if possible, several candidates must be sought and identified, who must be subjected to formalised assessments;
- possible situations of conflict of interest concerning candidates must be identified and assessed, if they are linked to Public Officers or hold or have held public offices;
- at the time of hiring, the validity of residence permits for workers from non-EU countries must be verified;
- all letters of commitment and appointment must be signed by parties with appropriate powers;
- debriefing interviews must be carried out for resigning personnel;

- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed are applied in the following reference document:

- P_STAFF01_GR “Employee Group Handbook –HR Procedure”
- "Guidelines for the management of relations with the Public Administration".

With reference to the “**Administrative management of personnel and reimbursement of expenses;**”, protocols establish that:

Personnel management

- all documents and formal communications concerning personnel must only be managed and signed only by parties with appropriate powers;
- the Unit Manager for the implementation of the operation must make sure that the documents, declarations and information sent to the relevant entities are complete and truthful;
- in relation to personnel belonging to protected categories, verification of any gaps must be ensured by monitoring and compliance with legal requirements and thresholds;
- specific controls are provided for to ensure the records of the staff costs are correct;
- periodic monitoring of the expiration dates of residence permits for workers from non-EU countries must be implemented, thereby requesting their renewal according to the legal deadlines;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Lists of expenses

- the management of business trips and the reporting of the related expenses must be carried out in compliance with the rules and operating procedures established by the relevant applicable procedures;
- according to the hierarchical levels present in the company, the Manager who authorises ex ante (depending on the type of business trips, missions or journeys outside the usual workplaces), the business trip and cash advances to the requesting parties must be identified;
- according to the hierarchical levels existing at the company, the Manager verifying and authorising lists of expenses submitted by employees must be identified;
- the use of the company credit card, if assigned, must be permitted in compliance with the rules specified by the relevant applicable procedures;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF01.GR “Employee Group Handbook – HR Procedure”;
- P_STAFF17.IT “Administrative and accounting procedure for Personnel management”;
- I_STAFF04.IT “Operating instruction for the allocation and management of company credit cards”;
- I_STAFF10.IT “Operating instruction for managing cash”
- "Guidelines for the management of relations with the Public Administration".

With reference to the **“Management of capital goods and company benefits (e.g. cars, mobile phones, personal computers, corporate credit cards, etc.)”** protocols establish that:

- operations must be carried out with the assistance of the HR & Organization Unit, also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- when acquiring capital goods and company assets, the specific prevention protocols are complied with, where applicable, governed under the area of Sensitive Activity "Management of purchases of goods and services";
- the assignment of the benefits must be justified, in relation to the company policies applied and based on the role and duties of the beneficiary personnel and conveyed by means of a formal request from the person concerned, validated by a superior;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF01.GR "Employee Group Handbook – HR Procedure";
- I_STAFF04.IT "Operating instruction for the allocation and management of company credit cards";
- P_FKRGRITA_N01_HR Procedure Management of company cars for mixed use Group - ITA"
- "Guidelines for the management of relations with the Public Administration".

With reference to transactions concerning the "**Management of gifts, gratuities, donations and sponsorship**", protocols establish that:

Gifts and gratuities

- the operations of the Company or subsidiaries must be managed with the assistance of the Communication & Stakeholder Engagement Unit, also by virtue of specific

intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;

- provided gifts must be of modest value and directly and exclusively related to business activities;
- in addition to being aimed at licit and ethical activities, operations must also be authorised, justified and documented;
- the types of goods/services offered, the relative value and the names and relative roles of the recipients must be informed;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Donations and sponsorships

- the operations of the Company or subsidiaries must be carried out with the assistance of the Stakeholder Engagement Communication Unit, also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- operations must be adequately justified and, in the case of sponsorship, aimed at increasing and promoting the image of the Company, in compliance with the ethical principles thereof;
- the transaction is approved by persons with the necessary powers;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- I_STAFF01.GR "Operating instruction for the management of gifts and presents";

- I_STAFF02.GR “Operating instruction for the management of donations and sponsorships”
- "Guidelines for the management of relations with the Public Administration".

With reference to the transactions regarding the "**Management of purchasing goods and services**" and the "**Assignment and management of fiduciary advice (legal, technical, notarial, tax)**", the protocols establish that:

- procurement activities must be carried out in compliance with the rules and operating procedures established by the relevant applicable procedures;
- the purchasing process must meet quality, professionalism, reliability and cost-effectiveness requirements, in compliance with transparency and impartiality principles;
- information must be provided about the procedure followed for the authorisation and performance of the purchase, as well as the purpose, amount and reasons underlying the choice of the supplier;
- the supplier qualification process must be aimed at certifying a database of selected parties for which the satisfaction of economic-financial, organisational, ethical-reputational and technical-managerial requirements have been verified and documented;
- the qualification process must require the assessment, among other things, (i) of subjective aspects of the counterparty (for example, the existence of criminal records, questionable reputation, admissions or statements by the counterparty regarding the involvement thereof in criminal activities, counterparties that use trust companies³ preventing the identification of the natural persons involved in the transaction); (ii) of the conduct of the counterparty (for example ambiguous behaviour, lack of data necessary for carrying out transactions or reticence in providing it; (iii) of the territorial

³ Identified according to the Italian Law 1966 of 23 November 1939 “Regulations of trusts and auditing companies”

spread of the counterparty (for example, transactions carried out in “non-cooperative” countries⁴;

- specific checks must be carried out in the event of offers to supply goods at prices significantly lower than market prices, aimed at verifying, as possible, the actual origin of the goods;
- there is a check made of the substantive and formal consistency of the invoice with respect to the goods delivered and/or service provided, and the presence in the invoice of the necessary indications regarding its registration;
- the procurement of goods or services must always be governed by a written agreement (order and/or contract), signed by parties with appropriate powers, clearly specifying the purpose of the contract and the price of the good or service or the criteria for determining it;
- the actual delivery of the goods or the provision of the services must be verified by the relevant Corporate Unit before payment is made;
- no fees or charges are paid to consultants in an amount that is not commensurate with the services rendered to the Company or that does not comply with the assignment given, the conditions or practices existing on the market or the professional rates in force for the category concerned;
- an economic-asset profile is also evaluated for each transaction (for example unusual transactions in terms of type, frequency, time frames, amount, geographic location) and the characteristics and purposes of the transaction (for example use of nominees -

⁴ The lists may be consulted through the link on the website of Italy's Financial Intelligence Unit (FIU) in the section, "Home / Combating the financing of terrorism and the activities of countries that threaten international peace and security", or, alternatively, directly at:

- http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm, for the list prepared by the European Union;
- <http://www.treas.gov/offices/enforcement/ofac/sdn/>, for the OFAC (Office of Foreign Assets Control - United States Department of the Treasury) List;
- http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml, for the list prepared by the United Nations.

including fiduciary and trust companies, amendments of the standard contractual terms, purpose of the transaction);

- contracts governing relations with consultants and suppliers must include a specific clause: (i) requiring an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Group's Code of Ethics and, as applicable, in the Company's Model; and (ii) stating the consequences in the event of a breach of that declared (including the termination of the contract itself);
- the produced, sent and received documentation that relates to the purchase of goods and services must be properly filed in a specific archive by the Corporate Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF05.GR "Purchasing procedure";
- P_STAFF04.GR "Procedure for managing legal activities";
- P_STAFF08.GR "Administrative and accounting procedure for the management of the Purchase Cycle";
- P_STAFF18.GR "Administrative and accounting procedure for managing fixed assets";
- "Guidelines for the management of relations with the Public Administration".

With reference to "**Commercial, marketing and business development management**", the protocols establish that:

- the commercial activities must be carried out in coordination with the Energy Management Division and Downstream Services Division also by virtue of specific

intercompany contracts and in compliance with the rules and operating procedures required by the relevant applicable procedures;

- in the management of current or potential customers, transparent relations must be maintained and no undue advantages, money or personal benefits may be offered to the representatives of the potential customers for negotiations to be successful (beyond customary courtesy and modest value limits);
- potential new customers must also be evaluated in terms of reliability and ethics, by collecting information about: (i) subjective aspects of the counterparty and its representatives (for example, existence of criminal records, questionable reputation, admissions or statements by the counterparty regarding its involvement in criminal activities, counterparties using trust companies preventing the identification of the natural persons involved in the transaction); (ii) the conduct by the counterparty (for example ambiguous behaviour, lack of data necessary for carrying out transactions or reticence in supplying it); (iii) the corporate structure upstream of the customer; (iv) economic-financial aspects of the transaction (for example, unusual transactions based on type, frequency, timing, amount and geographical location); (v) the territorial spread of the counterparty (for example, transactions carried out in “non- cooperative” countries);⁵
- all documents, requests and formal communications, which are intended for customers must be managed and signed only by previously identified and authorised persons;

⁵ The lists may be consulted through the link on the website of Italy's Financial Intelligence Unit (FIU) in the section, "Home / Combating the financing of terrorism and the activities of countries that threaten international peace and security", or, alternatively, directly at:

- http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm, for the list prepared by the European Union;
- <http://www.treas.gov/offices/enforcement/ofac/sdn/>, for the OFAC (Office of Foreign Assets Control - United States Department of the Treasury) List;
- http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml, for the list prepared by the United Nations.

- controls are provided so that the revenues resulting from commercial, marketing and business development activity are determined with respect to existing operations/transactions;
- contracts governing relations with customer must include a specific clause: (i) requiring an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Group's Code of Ethics; and (ii) stating the consequences in the event of a breach of that declared;
- the traceability of the decision-making processes and the assessments carried out must be ensured, with reference to: (i) the possession of the expertise and resources necessary for the management of the contract, with respect to the activities requested by the customer; (ii) the powers and authorisations necessary to fulfil that ordered by the customer and any situations of conflict of interest; (iii) required clauses and guarantees;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Additional safeguards applicable in the performance of marketing and corporate website management activities

- promotion and organisation (or participation) of (a) events, conferences and congresses must be approved by parties with appropriate powers;
- the works protected by copyright purchased by the Company for the purposes of communication and/or marketing must be catalogued in a database that includes the following data:
 - list/description of images, musical or other intellectual works for which user licences have been acquired
 - date of purchase of the licence

- date of expiry of the licence
- type of use authorised by the licence agreement (e.g. uploading on the website, public dissemination, use for brochure and the maximum number of copies that can be used, etc.);
- methods and procedures for checking the users' access to content download sites must be specified and implemented;
- controls on activities involving the use of intellectual property must be envisaged;

Further controls applicable if business agents/mediators are used

- the reputation, professionalism, expertise, independence and reliability of the party on the market, as well as the absence of conflicts of interest must be assessed in advance upon choosing a business promoter/broker;
- the service must be governed by a written agreement, clearly specifying the following: (i) the purpose, nature and timing of rendering the service, (ii) the structure of the fees, and (iii) the amount of the fees or the criteria for determining them;
- contracts with business promoters/brokers must be entered into exclusively by authorised subjects and in compliance with the system of powers in force;
- contracts governing relations with business promoters/brokers must include a specific clause: (i) requiring an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Group's Code of Ethics and, as applicable, in the Company's Model; (ii) stating the consequences in the event of a breach of that declared (including the termination of the contract itself).

The specific prevention protocols listed above are applied in the following relevant documents:

- P_BUSLN03.GR "Procedure for managing Energy Management & Downstream Services activities";
- P_STAFF04.GR "Procedure for managing legal activities";

- P_STAFF16.GR “Administrative and accounting procedure for the management of the Sales Cycle”;
- I_STAFF12.GR “Operating instruction for the management of relations with the Public Administration”
- "Guidelines for the management of relations with the Public Administration".

B. COMPUTER CRIMES AND UNLAWFUL DATA PROCESSING (ARTICLE 24-BIS OF THE DECREE)

B.1 Applicable offences

Based on the analyses carried out, the following computer crimes are considered as applicable to the Company:

- **forgery of electronic documents**, envisaged by Article 491-bis of the Italian Criminal Code and identifiable in the material and ideological forgery cases committed on public documents, certificates, by a representative of the Public Administration, if their subject-matter is a “public electronic document with probatory efficacy”. “Electronic document” means the electronic representation of deeds, facts or data legally relevant that has evidential value (this crime extends the criminal prosecution of the offences provided for in Book II, Title VII, Chapter III of the Italian Criminal Code to electronic documents with probatory efficacy);
- **computer or telematic hacking**, envisaged by Article 615-ter of the Italian Criminal Code and identifiable whenever anyone accesses improperly - i.e. by eluding any minimum form of impedimental barrier - an IT or telematic system protected by security measures, or remains there against the will of whoever has the right to exclude him/her;
- **unauthorised possession and dissemination of access codes to IT or telematic systems**, envisaged by Article 615-quarter of the Italian Criminal Code and identifiable whenever anyone obtains, reproduces, disseminates, communicates or delivers illegally codes, passwords or other appropriate means to access an IT or telematic system protected by security measures, or otherwise provides information or instructions in this sense, in view of procuring oneself or others a profit, or causing others a damage;
- **dissemination of equipment, devices or software intended to damage or disrupt an IT or telematic system**, envisaged by Article 615-quinquies of the Italian Criminal Code that punishes the behaviour of those who, in order to damage illegally an IT or telematic

system, or information, data or programmes contained or relevant thereto, or to facilitate the interruption or alteration of its operation, procure, produce, reproduce, import, disseminate, communicate, deliver, or however make available to others equipment, devices or computer programmes;

- **illegal tapping, impediment or disruption of IT communications or telecommunications** envisaged by Article 617-quarter of the Italian Criminal Code that punishes the behaviour of those who fraudulently intercept communications concerning an IT or telematic system or across multiple systems, prevent or interrupt them or reveal, through any means of public disclosure, in whole or in part, the contents of these communications;
- **installation of equipment designed to tap, prevent or disrupt IT communications or telecommunications** envisaged by Article 617-quinquies of the Italian Criminal Code that punishes the behaviour of those who, outside the cases permitted by law, install equipment designed to tap, prevent or disrupt communications concerning an IT or telematic system, or across multiple systems;
- **damage to information, data and computer programmes** envisaged by Article 635- bis of the Italian Criminal Code and identifiable whenever anyone destroys, damages, cancels, alters or removes information, data or computer programmes of others, save that the fact constitutes a more serious offence;
- **damage to information, data and computer programmes used by the State or other public entity, or however of public interest** envisaged by Article 635-ter of the Italian Criminal Code and identifiable whenever anyone commits a fact in order to destroy, damage, cancel, alter or remove information, data or computer programmes used by the State or other public entity or pertaining thereto, or however of public interest, save that the fact constitutes a more serious offence;
- **damage to IT or telematic systems** envisaged by Article 635-quarter of the Italian Criminal Code and identifiable whenever anyone, through the ways of behaviour set forth in Article 635-bis of the Italian Criminal Code, i.e. through the introduction or

transmission of data, information or programmes, destroys, damages, makes IT or telematic systems of others totally or partially unserviceable or seriously hampers their operation, save that the fact constitutes a more serious offence;

- **damage to IT or telematic systems of public interest** envisaged by Article 635-quinquies of the Italian Criminal Code and identifiable whenever anyone behaves as described in Article 635-quarter above of the Italian Criminal Code, if it is intended to destroy, damage, make IT or telematic systems of public interest totally or partially unserviceable or seriously hamper their operation;

B.2 Sensitive Activity

The Company identified the Sensitive Activity that can be carried out in its own interest and/or in the interest of a subsidiary within the scope of which, potentially, some of the offences envisaged by Article 24-bis of the Decree could be committed:

- management of IT systems.

B.3 Specific prevention protocols and respective implementation

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For operations concerning the "**management of IT systems**", the protocols specify that:

Management of logical accesses

- the operations of the Company must be managed with the assistance of the Digital Transformation & IT Unit, also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- system authentication requirements for data access and for assigning remote access to the systems by third parties such as consultants and suppliers must be formally defined;

- the identification codes (user-id) for accessing applications and the network must be individual and unique (with the exception of users used in the context of special services);
- proper password management must be defined by the guidelines, sent to all users for selecting and using the password;
- the methods and procedures for the creation of passwords to access the network, applications, business information assets and critical or sensitive systems must be defined (for example minimum password length, rules of complexity, expiry);
- accesses made by users, in any manner, to data, systems and network must be regularly monitored;
- applications must keep track of changes to data made by users (where applicable);
- methods and procedures for assigning, changing and cancelling user profiles must be defined;
- an (application/profile/applicant) authorisation matrix periodically aligned with the existing organisational roles and consistent with the principles of role segregation must be prepared;
- periodic checks of user profiles must be carried out in order to check that they are consistent with the responsibilities assigned and with the principles of role segregation;
- documents concerning each relevant activity must be filed in order to ensure complete traceability;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Management of the network infrastructure

- the operations of the Company must be managed with the assistance of the Digital Transformation & IT Unit, also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- the responsibilities for the management of networks must be defined;

- security controls must be implemented in order to ensure the confidentiality of data within the network and in transit over public networks;
- mechanisms must be adopted for the segregation of networks and the monitoring of network traffic;
- mechanisms must be implemented for tracking security events (or services) on servers (e.g., anomalous accesses in terms of frequency, method, timing);
- the implementation and maintenance of telematic networks must be regulated through the definition of responsibilities and operating methods, periodic checks on the operation of networks and on anomalies found;
- documents concerning each main activity must be filed in order to ensure complete traceability;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Management of hardware and software

- the operations of the Company must be managed with the assistance of the Digital Transformation & IT Department of Renantis S.p.A., also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the relevant applicable procedures;
- the methods and procedures for managing servers for the drawing-up and maintenance of an up-to-date inventory of the servers used by the Company and that regulate the responsibilities and operating methods in case of implementation and/or maintenance of hardware must be defined;
- the backup methods and procedures establishing, for each hardware application, the frequency of the activity, procedures, number of copies and data storage period must be defined;
- the methods and procedures for managing the main software systems for the drawing-up and maintenance of an up-to-date inventory of the software used by the company, for using formally authorised and certified software and for carrying out periodic checks

on the installed software and on the used system memories to monitor the presence of prohibited, unlicensed and/or potentially harmful software must be defined;

- if management is outsourced, contracts regulating relations with service providers must be subject to clauses that require:
 - the compliance of the software supplied with laws and regulations and in particular with the provisions of Italian Law no. 633 of 22 April 1941
 - the Company to be held harmless in case of violations committed by the service providers themselves;
- applications must keep track of changes to data and systems made by users;
- a business continuity plan and a disaster recovery plan must be defined at the level of IT systems;
- the criteria and methods for change management (understood as the updating or implementation of new technological systems/services) must be defined;
- physical access credentials to sites where information systems and IT infrastructures reside such as, by way of example, badges and their traceability, must be defined;
- the adopted security measures, the methods of surveillance and their frequency, the responsibility, the process of reporting violations/forced entry of technical rooms or breaches of security measures, the countermeasures to be activated must be defined;
- documents concerning each activity must be filed in order to ensure their complete traceability;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- IT Policy Framework;
- IT Tools Management Policy;
- Monitoring Procedure and Security Systems Control;
- Monitoring Procedure and third party control;

- Logical Access Management Procedure;
- Information Security Policy;
- Disaster Recovery Infrastructure;
- Patch Management;
- Request for access to Office 365 resources and assignment of roles;
- Cybersecurity KPIs;
- Asset IT Management;
- Backup Management;
- Cybersecurity Model;
- "Data Protection Policy" published on the Intranet of the Company under the Governance & Compliance section of the company Intranet.

C. ORGANISED CRIME AND TRANSNATIONAL OFFENCES (ARTICLE 24-TER OF THE DECREE AND ARTICLE 10, ITALIAN LAW NO. 146 OF 16 MARCH 2006.)

C.1 Applicable offences

Based on the analyses carried out, the following organised crime and transnational offences are considered as applicable to the Company:

- **criminal conspiracy, envisaged by Article 416 of the Italian Criminal Code and that punishes those who promote, constitute or organise an association made up of three or more persons with the aim of committing several crimes, as well as those who participate in it;**
- **association with the Mafia including at international level, envisaged by Article 416-bis of the Italian Criminal Code and that punishes whoever is part of an association with the Mafia made up of three or more persons as well as those who promote, manage or organise it.** The association is of mafia type when those taking part in it make use of the intimidating power of their association and of the condition of subjugation and silence that comes from it to commit crimes, to directly or indirectly acquire the management or control of economic activity, concessions, authorisations, tenders and public services or to make unjust profits or advantages for themselves or for others or to impede or obstruct the freedom of vote, or to obtain votes for themselves or for others on the occasion of elections. The association is considered armed when the participants have availability of weapons or explosive materials for the achievement of the purpose of the association, even if concealed or kept in a repository. The provisions of Article 416-bis also apply to the 'Camorra' (mafia-style criminal organisation in the Campania region of Italy) and to the other associations, however locally denominated, including at international level, which by making use of the intimidating power of their association, pursue aims corresponding to those of mafia-style associations;
- **crimes committed by making use of the conditions envisaged by Article 416-bis of the Italian Criminal Code or in order to facilitate the activities of associations envisaged**

by the same article;

- political and mafia-related vote-rigging, established by art. 416-ter of the Italian Criminal Code, which punishes: i) anyone who accepts a promise to obtain votes by the methods referred to in paragraph three of article 416-bis in exchange for the provision or the promise to provide money or other benefits; ii) anyone who promises to obtain votes in the manner described above.
- **incitement not to make statements or to make false statements in court** envisaged by Article 377-bis of the Italian Criminal Code and identifiable whenever anyone, with violence or threat, or with offer or promise of money or other benefits, incites the person required to make before the court statements that can be used in criminal proceedings not to make statements or to make false statements in court, when this person has the right to silence;
- **aiding and abetting** envisaged by Article 378 of the Italian Criminal Code and identifiable whenever anyone, after the commitment of a crime for which the law establishes the death penalty or life imprisonment or imprisonment, and except for the cases of complicity in the same, helps individuals to circumvent the authority's investigations, or to evade the authority's searches.

C.2 Sensitive Activity

The crimes set forth in Article 24-ter of the Decree and set forth in Article 10, Italian Law no. 146 of 16 March 2006, do not appear to be related to specific activities actually carried out by the Company, in its own interest and/or in the interest of a subsidiary by virtue of specific intercompany contracts. Moreover, it must be noted that:

- these crimes are, for the most part, offences of association (criminal conspiracy, mafia-style association including at international level) or strongly related to offences of association (crimes committed using the methods set out in Article 416-bis of the Italian Criminal Code or in order to facilitate the activity of the associations envisaged by it),

which therefore punish even the agreement of several people to commit an indefinite number and type of crimes;

- since, by definition, the offences of association consist of the agreement aimed at committing any crime, they extend the number of predicate offences to an unspecified number of criminal figures, for which any activity carried out by the Company could involve the commission of a crime - and the consequent liability pursuant to Italian Legislative Decree 231/2001 - “through” criminal conspiracy.

However, although such offences are, as mentioned above, not attributable to specific activities actually carried out by the Company - and, therefore, to the related operating procedures - they may be committed in the abstract by both Senior individuals and Subordinate Individuals. With reference to this aspect, the prevention system already in place in the Company becomes important. In fact, it was considered that, for the prevention of these offences, the existing corporate governance structures, as well as the principles contained in the Code of Ethics, which constitute the most suitable tool for offences such as criminal conspiracy set forth in Article 416 of the Italian Criminal Code, can perform an adequate preventive function, due to the impossibility of classifying within a specific control system the almost infinite number of offences that could be committed through associations. Nevertheless, the Company has in any case identified a series of activities in which subjects referring to criminal associations, or who in any case carry out unlawful activities, can come into contact and manage business activities with the Company itself. In particular, the following Sensitive Activity have been identified, within which, certain organised crime envisaged by Article 24-ter of the Decree and certain transnational offences envisaged by Article 10 of Italian law no. 146 of 16 March 2006 could be potentially committed:

- management of relations with the Public Administration, including, but not limited to, (i) requests for opinions, authorisations, licences or authorisations for the acquisition / development / construction / operation of energy production plants with renewable and non-renewable sources, (ii) inspections, (iii) energy efficiency improvement for buildings and public roads including “smart” energy management;

- activities to acquire/establish rights in areas owned by local/private bodies, to be allocated to the development/construction of energy production plants with renewable and non-renewable sources and expropriation procedures;
- treasury, payments and funds management for the Company;
- management of intercompany relations;
- management of disputes;
- management of purchases of goods and services;
- personnel selection, recruitment and development;
- sales, marketing and business development management.

C.3 Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For transactions regarding the **“ Management of relations with the Public Administration, including, but not limited to, (i) requests for opinions, authorisations, licences or authorisations for the acquisition / development / construction / operation of energy production plants with renewable and non-renewable sources, (ii) inspections, (iii) energy efficiency improvement for buildings and public roads including “smart” energy management, “Activities to acquire/ establish rights in areas owned by local/ private bodies, to be allocated to the development/ construction of energy production plants with renewable and non-renewable sources and expropriation procedures”, “Management of disputes”, “Management of purchases of goods and services” and the “ Establishment of rights in rem and rights to use land set aside for the construction of renewable energy production plants”, “Personnel selection, recruitment and development”, “Sales, marketing and business development management”, “Management of the treasury, payments and financial resources of the Company” and the “Management of the treasury,**

payments and financial resources of the Company", the provisions of the prevention protocols and relevant procedures as per paragraph A.4 of this Special Part, with reference to the corresponding Sensitive Activity, shall apply.

D. CRIMES AGAINST INDUSTRY AND TRADE (ARTICLE 25-BIS.1 OF THE DECREE)

D.1 Applicable offences

On the basis of the analyses conducted, the following crime against industry and trade is considered applicable to the Company: manufacture and trade of goods produced in encroachment of industrial ownership rights, envisaged by Article 517-ter of the Italian Criminal Code and punishes whoever, without prejudice to the application of Articles 473 and 474 of the Italian Criminal Code, being able to know of the existence of the industrial property rights, manufactures or uses industrially objects or other goods produced in encroachment of an industrial ownership right or in violation thereof, as well as whoever, for profit, introduces within the State, holds for sale, offers for sale directly to consumers or puts these goods into circulation.

D.2 Sensitive Activity

The Company identified the following Sensitive Activity that can be carried out in its own interest and/or in the interest of a subsidiary by virtue of specific intercompany contracts within which, potentially, the above-mentioned crime against industry and trade envisaged by Article 25-bis.1 of the Decree could be committed: plant design and construction for subsidiaries.

D.3 Specific prevention protocols

For operations concerning plant design and construction for subsidiaries, the protocols specify that:

- the process must be formalised by an operational procedure or internal policy;
- the truthfulness and correctness of the documents supporting the inspections carried out must be checked and their storage guaranteed;
- there must be no subjective identity between those who deal with the design and implementation and those who deal with quality control, including compliance with any licenses and/or patents.

D.4 Implementation of specific prevention protocols

The specific prevention protocols listed above are applied in the following Group documents:

- P_BUSLN04.GR “Procedure for managing Performance & Technical Innovation activities”;
- P_BUSLN03.GR “Procedure for specifying and safeguarding Energy Management & Downstream Services activities”;
- P_BUSLN02.GR “Procedure for Engineering & Construction activities”;
- P_STAFF04.GR “Procedure for managing legal activities”;
- P_STAFF05.GR “Purchasing procedure”;
- P_STAFF02.GR “Procedure for defining and monitoring Information Technology activities”;
- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”.

E. CORPORATE OFFENCES (ARTICLE 25-TER OF THE DECREE)

E.1 Applicable offences

Based on the analyses carried out, the following corporate offences are considered as applicable to the Company:

- fraudulent corporate communications, envisaged by Article 2621 of the Italian Civil Code, are identifiable whenever directors, general managers, executives in charge of preparing the company's accounting documents, auditors and liquidators, and in order to obtain for themselves or others an unfair profit, in financial statements, reports or other corporate communications required by law, intended for shareholders or the public, knowingly represent relevant material facts not true to life or omit relevant material facts, the disclosure of which is compulsory by law on the economic or financial situation of the Company or group to which it belongs, which can actually lead it to mislead the recipients on the above-mentioned situation. The liability to punishment is also extended in the event in which the fraud or the omissions concern assets owned or administered by the Company on behalf of third parties;
- **obstructed control**, envisaged by Article 2625 of the Italian Civil Code and identifiable whenever directors impede or hamper the control by shareholders or other corporate bodies, by hiding documents or through other appropriate stratagems, causing damage to the shareholders;
- **undue return of contributions**, envisaged by Article 2626 of Italian Civil Code and identifiable whenever directors, except in cases of lawful reduction of share capital, return, also fictitiously, the contributions to shareholders or exempt them from the obligation of making contributions;
- illegal distribution of profits and reserves, envisaged by Article 2627 of the Italian Civil Code and identifiable whenever directors distribute profits or advances on profits not actually realised or destined by law to reserve, or distribute reserves, also not made up of profits, which cannot be distributed by law;

- **unlawful transactions on shares of the parent company**, envisaged by Article 2628 of the Italian Civil Code and identifiable whenever directors, outside of the cases allowed by law, acquire or subscribe shares, causing damage to the wholeness of the share capital or the reserves not distributable by law; or outside of the cases allowed by law, acquire or subscribe shares or shares issued by the parent company, causing damage to the share capital or the reserves not distributable by law;
- **transactions to the detriment of creditors**, envisaged by Article 2629 of the Italian Civil Code and identifiable whenever directors, in violation of the legal provisions to protect creditors, reduce the share capital or carry out mergers with other company or demergers, causing damage to the creditors;
- **fictitious capital formation**, envisaged by Article 2632 of the Italian Civil Code and identifiable whenever directors and contributing shareholders, either in whole or in part, fictitiously form or increase the share capital through allocations of shares in an overall amount greater than the amount of the share capital, mutual subscription of shares, overvaluation of non-cash contributions or of receivables or equity of the company in the event of transformation;
- **illicit influence on the general shareholders' meeting**, envisaged by Article 2636 of the Italian Civil Code and identifiable whenever anyone, with fictitious or fraudulent actions, determines the majority in the shareholders' meeting, with the aim of procuring an unfair profit for oneself or others;
- **market rigging**, envisaged by Article 2637 of Italian Civil Code and identifiable whenever anyone disseminates false information or carries out simulated transactions or other stratagems specifically suitable to cause a considerable change in the price of unlisted financial instruments or for which no request was submitted for admission to trading on a regulated market, or to significantly impact the confidence of the public in the financial stability of banks or banking groups;
- **obstacle to the exercise of public supervisory authority functions**, envisaged by Article 2638 of the Italian Civil Code and identifiable whenever directors, general managers,

executives in charge of preparing the company's accounting documents, auditors and liquidators of companies or entities and other subjects who are legally subject to the public supervisory authorities or bound by obligations towards them, in the communications to the aforesaid authorities provided on the basis of the law, in order to obstruct the exercise of the supervisory functions, represent material facts not true to life albeit assessed, on the economic or financial situation of those subject to supervision or, with the same purpose, conceal by other fraudulent means, in whole or in part, facts that should have been communicated, concerning the situation itself, also if the information concerns assets owned or managed by the Company on behalf of third parties; or whenever directors, general managers, auditors and liquidators of companies or entities and other subjects who are legally subject to the supervisory public entities or bound by obligations towards them, in any form whatsoever, also by omitting communications due to the aforesaid authorities, knowingly obstruct their functions;

- **corruption in the private sector and incitement to corruption**, refer to paragraph L. “Corruption in the private sector” that deals with it (and identifies its Sensitive Activity and related Specific prevention protocols).

E.2 Sensitive Activity

The Company identified the Sensitive Activity that can be carried out in its own interest and/or in the interest of a subsidiary also by virtue of specific intercompany contracts within which, potentially, some of the corporate offences envisaged by Article 25-ter of the Decree could be committed:

- management of relations with the Public Administration, including, but not limited to, requests for opinions, authorisations, licences or authorisations for the construction and operation of energy production plants with renewable sources, (ii) inspections, (iii) energy efficiency improvement for buildings and public roads including “smart” energy management;

- management of corporate affairs and extraordinary transactions;
- management of intercompany relations;
- preparation of financial statements, interim financial statements, reporting packages and any prospectuses, preparation of any other external communication addressed to the financial markets or to any other party (e.g. the media and the press);
- management of relations with Shareholders, the auditing company and the Management Control Committee;
- keeping of documents over which other company bodies could exercise control (e.g. corporate books);
- preparation of documents for the purposes of resolutions of the Shareholders' Meeting and the Board of Directors;
- bookkeeping, financial statements management and periodic reporting;
- tax management.

E.3 Specific prevention protocols

For transactions regarding the “ **Management of relations with the Public Administration, including, but not limited to, (i) requests for opinions, authorisations, licences or authorisations for the acquisition / development / construction / operation of energy production plants with renewable and non-renewable sources, (ii) inspections, (iii) energy efficiency improvement for buildings and public roads including “smart” energy management** ”, “**Activities to acquire/ establish rights in areas owned by local/ private bodies, to be allocated to the development/ construction of energy production plants with renewable and non-renewable sources and expropriation procedures**”, the “**management of corporate affairs and extraordinary transactions**” and the “**management of intercompany relations**” the provisions of paragraph A.4 with reference to the corresponding Sensitive Activity shall apply.

For operations concerning the preparation of financial statements, interim financial statements, reporting packages and any prospectuses; preparation of any other external communication addressed to the financial markets or to any other party, the protocols specify that:

- an accounting manual, constantly updated, which clearly indicates the data and information that each Corporate Unit must provide, the accounting methods of data and timing in order to send them to the responsible Corporate Units and service providers involved must be adopted;
- all recognition and recording operations of business activities must be carried out with correctness and in compliance with the principles of truthfulness and completeness;
- the different Corporate Unit Managers must provide the CFO with the information requested of them in a timely manner and certifying, where possible, the completeness and truthfulness of the information, or indicating the persons who may provide such certification;
- where it is useful for the understanding of the information, the managers must indicate the original documents or sources from which the information sent is taken and processed, and, where possible, must attach a copy thereof;
- the collection, transmission and aggregation of accounting information for the purpose of preparing corporate communications must be carried out exclusively by means of methods that can guarantee the traceability of the individual steps of the data formation process and the identification of the subjects who enter the data into the system; access profiles to this system must be identified by the Corporate Unit in charge, with the support of the HR & Organization Unit, so as to ensure the segregation of duties and consistency of authorisation levels;
- any changes to the financial statement items or to their accounting methods must be authorised by the CFO and its Corporate Units, with the involvement of service providers, where present;

- the request by anyone for unjustified changes in the recognition, recording and accounting representation or for quantitative changes of figures compared to those already recognised on the basis of the Company's operating procedures, must be immediately notified to the Supervisory Body;
- the draft financial statements and other accounting documents must be made available to the directors well in advance of the meeting of the Board of Directors called to approve the financial statements;
- if the management of this activity or part of it is outsourced, contracts regulating relations with service providers must be subject to clauses referring to the fulfilments and responsibilities deriving from the Decree and from compliance with the main principles of the Code of Ethics, which are communicated to them in accordance with paragraph 6 of the General Part and which indicate clear contractual effects with regard to failure to comply with such fulfilments.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF08.GR “Administrative and accounting procedure for the management of the Purchase Cycle”;
- P_STAFF12.GR “Administrative and accounting procedure for the management of court and out-of-court disputes”;
- P_STAFF13.GR “Administrative and accounting procedure for managing corporate affairs”;
- P_STAFF14.GR “Administrative and accounting procedure for the preparation of the Consolidated Financial Statements”;
- P_STAFF15.GR “Administrative and accounting procedure for the management of hedges against financial risks”;
- P_STAFF16.GR “Administrative and accounting procedure for the management of the Sales Cycle”;
- P_STAFF17.IT “Administrative and accounting procedure for Personnel management”;

- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”;
- P_STAFF19.GR “Administrative and accounting procedure for the management of financial accounting and treasury activities”;
- P_STAFF20.GR “Administrative and accounting procedure for the management of closing of the accounts and preparation of the financial statements”;

For operations concerning the **“Management of relations with Shareholders, the auditing company and the Management Control Committee, the keeping of documents over which other company bodies could exercise control and the preparation of documents for the purposes of resolutions of the Shareholders' Meeting and the Board of Directors”**, the protocols specify that:

- a company Manager who is responsible for the collection and processing of the information requested and sent to the Management Control Committee and to the auditing company, after checking its completeness, relevance and correctness must be identified for each Function;
- the transmission of data and information, as well as any finding, communication or evaluation officially expressed by the Shareholders, the Management Control Committee and the auditing company, must be documented and kept;
- all documents relating to operations on the agenda of the Shareholders' Meeting or the Board of Directors or, in any case, relating to operations on which the Management Control Committee or the auditing company must express an opinion or formulate a report, must be communicated and made available well in advance of the date of the meeting;
- the methods for selecting assessing and appointing the auditing company must be formalised;
- the auditing company, the Management Control Committee and the Shareholders must be guaranteed free access to the company's accounts and all other information required for the correct carrying-out of their task.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF13.GR “Administrative and accounting procedure for managing corporate affairs”;
- I_STAFF07.GR “Operating instruction for reporting to the Board of Directors and the Board of Statutory Auditors of Renantis S.p.A.”

For operations regarding the "**Bookkeeping, financial statements management and periodic reporting**", the protocols provide that;

- the operations of the Company must be managed with the assistance of the Administration company structure, also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures established by the applicable administration-accounting procedures;
- constantly updated procedures clearly indicating the data and information that each Corporate Unit must provide, the accounting methods of data and timing in order to send them to the Corporate Unit in charge and service providers involved must be adopted;
- all recognition and recording operations of business activities must be carried out with correctness and in compliance with the principles of truthfulness, existence, competence and completeness;
- the general bookkeeping and the drawing up of the financial statements will be carried out in accordance with the Civil Code and applicable accounting standards;
- the collection, transmission and aggregation of accounting information for the purpose of preparing corporate communications must be carried out exclusively by means of methods that can guarantee the traceability of the individual steps of the data formation process and the identification of the subjects who enter the data into the system;

- the system access profiles are defined in a way that guarantees the separation of the functions and the consistency of the authorisation levels;
- any changes to the financial statement items or to their accounting methods must be authorised by the Chief Executive Officer, with the involvement of service providers, where present;
- the draft financial statements file will be approved by the Chief Executive Officer of the Company before being submitted to the Board of Directors;
- the draft financial statements and other accounting documents must be made available to the directors well in advance of the meeting of the Board of Directors called to approve the financial statements;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_STAFF08.GR “Administrative and accounting procedure for the management of the Purchase Cycle”;
- P_STAFF12.GR “Administrative and accounting procedure for the management of court and out-of-court disputes”;
- P_STAFF13.GR “Administrative and accounting procedure for managing corporate affairs”;
- P_STAFF14.GR “Administrative and accounting procedure for the preparation of the Consolidated Financial Statements”;
- P_STAFF15.GR “Administrative and accounting procedure for the management of hedges against financial risks”;
- P_STAFF16.GR “Administrative and accounting procedure for the management of the Sales Cycle”;

- P_STAFF17.IT “Administrative and accounting procedure for Personnel management”;
- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”;
- P_STAFF19.GR “Administrative and accounting procedure for the management of financial accounting and treasury activities”;
- P_STAFF20.GR “Administrative and accounting procedure for the management of closing of the accounts and preparation of the financial statements”;

For activities concerning the "**tax management**", the protocols specify that:

- the assessment of the tax aspects related to the Company’s operations must be carried out with the support of the Tax Unit also by virtue of specific intercompany contracts;
- the tax requirements are carried out in accordance with the methods and expiries provided for under applicable laws;
- the accounting transactions involved in the determination of taxable income must be recorded in a truthful, correct and complete manner and in compliance with inherency principles and on an accrual basis, as well as being supported by suitable documentary evidence allowing for an accurate reconstruction;
- calculation of taxes is adequately tracked;
- periodic tax statements and notifications are prepared on a truthful, accurate and complete basis;
- tax statements and notifications are signed by the parties who have the necessary powers and are sent to the tax authorities in accordance with the methods and terms provided for by law;
- interim and balance tax amounts must be paid in compliance with the deadlines set by law;
- transactions to or from countries that are not considered to be "cooperative"⁶ must be adequately tracked and assessed;

⁶ Countries that "threaten international security" or alternatively, directly to the internet addresses:

- any relevant tax aspects concerning extraordinary transactions or intercompany transactions must be evaluated in advance and submitted to the attention of the relevant Corporate Units;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

-
- http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm, for the list prepared by the European Union;
 - <http://www.treas.gov/offices/enforcement/ofac/sdn/>, for the OFAC (Office of Foreign Assets Control - United States Department of the Treasury) List;
 - http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml, for the list prepared by the United Nations.

F. CRIMES AGAINST THE INDIVIDUAL (ARTICLE 25-QUINQUIES OF THE DECREE)

F.1. Applicable offences

Based on the analyses carried out, the following crime against the individual is considered applicable to the Company:

- **enslavement**, envisaged by Article 600 of the Italian Criminal Code and identifiable whenever anyone exercises powers on a person corresponding to those of the right of ownership or reduces to or keeps a person in a state of continued subjection, forcing him/her into work or sexual activity or begging or, however, into services that involve exploitation.

The reduction to or keeping in a state of subjection occurs when the behaviour is carried out with violence, threat, deceit, abuse of authority or taking advantage of a state of physical or mental inferiority or a situation of need, or by promise or offer of amounts of money or of other benefits to those who have authority over the person.

The following offence is also applicable:

- **illegal intermediation and labour exploitation**, envisaged by Article 603 bis of the Italian Criminal Code and identifiable whenever anyone (i) recruits labour for the purpose of working for third parties under exploitation conditions, (ii) uses, hires or employs labour, subjecting workers to conditions of exploitation and taking advantage of their state of need.

This offence occurs where recruitment takes place by taking advantage of the worker's state of need. The satisfaction of one or more of the following conditions constitute an indicator of exploitation: (i) repeated payment of wages in a manner that is clearly not in compliance with the national or local collective labour agreements signed by the most representative trade unions at national level, or in any event disproportionately low compared to the quantity and quality of the work performed; (ii) repeated violation of regulations on working hours, rest periods, weekly rest, compulsory leave and holidays; (iii) violations of regulations on safety and health at work (iv) the worker is subject to poor working conditions, surveillance methods or housing situations.

F.2 Sensitive Activity

The Company identified the following Sensitive Activity that can be carried out in its own interest and/or in the interest of a subsidiary by virtue of specific intercompany contracts within which, potentially, the above-mentioned crimes against the individual envisaged by Article 25-quinquies of the Decree could be committed: management of activities involving direct or indirect use of labour.

F.3 Specific prevention protocols

For operations entailing the management of activities involving direct or indirect use of labour, the provisions of the prevention protocols as per paragraph A.4 of this Special Part shall apply, with reference to the management of goods and services purchasing and administrative management of staff, expenses reimbursement and personal selection, recruitment and development.

G. CULPABLE HOMICIDE OR GRIEVOUS OR VERY GRIEVOUS HARM COMMITTED IN VIOLATION OF THE RULES ON PROTECTION OF HEALTH AND SAFETY AT WORK (ART. 25-SEPTIES OF THE DECREE)

G.1 Applicable offences

Based on the analyses carried out, crimes of culpable homicide or grievous or very grievous harm, committed with the violation of accident prevention regulations and of laws on the protection of health and the workplace are considered as applicable to the Company.

Articles 589 and 590, paragraph 3 of the Italian Criminal Code, referred to by Article 25-septies of the Decree, punish whoever, by negligence, causes the death of a person or causes grievous or very grievous harm, respectively 7.⁷

“Harm” means all the pathological effects constituting poor health, i.e. biological and functional disorders resulting from the occurrence of violent conduct: the harm is grievous if the poor health has endangered the victim’s life, has resulted in a period of convalescence exceeding forty days, or has led to the permanent weakening of the functional potential of a sense or an organ. The harm is very grievous if the behaviour has led to a probably incurable disease (with permanent incurable effects) or has caused the total loss of a sense, of a limb, of the ability to speak correctly or to procreate, the loss of the use of an organ or has disfigured or slashed the face of the victim.

The harmful event, whether represented by the grievous or very grievous harm or by death, can be committed by an active behaviour (the agent gives rise to a behaviour that damages the physical well-being of another person), or by means of an omissive conduct (the agent simply does not intervene to prevent the harmful event which he or she has a legal duty to prevent). A person is only liable for his or her own omissive behaviour that is harmful to the life or physical integrity of a person if he or she has a guarantee position towards the victim (i.e. if he or she has a legal duty to prevent the harmful event), which may be based on a contract or on the unilateral will of the agent. The legal system identifies the employer 8 as the guarantor “of the physical well-being and of the moral personality of the employees” and

its position of guarantee is however transferable to other subjects 9, on condition that the related delegation is sufficiently specific, prepared by means of a written deed and suitable for transferring all the authoritative and decision-making powers required to protect the safety of the employees.⁸⁹ The person chosen to hold the position must also be an eligible person qualified for the subject matter of the transfer of responsibility. Therefore, normally, an active behaviour will be recognised in the subject who carries out directly operational tasks and who materially harms others, whereas the omissive behaviour will be normally recognised in the subject who fails to comply with the supervisory and control obligations (e.g. employer, manager, person in charge) and thus does not intervene to prevent the event. From a subjective perspective, culpable homicide or relevant harm for the purposes of the administrative liability of entities must result from negligence: this subjective element can be general (violation of rules of behaviour crystallised in the social fabric under the rules of experience based on the parameters of diligence, prudence and expertise) or specific (violation of rules of behaviour positivized in laws, regulations or orders). In this regard, there is a profound difference with respect to the established subjective elements to be met for the other types of offenders referred to by the Decree, all punished on the basis of wilful malice: in such cases it is necessary for the subject to act on his/her own behalf and with the intent to produce the event-consequence based on own criminal conduct, imprudent or imperious behaviour in relation thereto not being sufficient.

In accordance with the Decree, the damaging behaviour of the agent that integrates the crimes of culpable homicide or grievous or very grievous harm must necessarily be aggravated, i.e. result in the violation of accident-prevention regulations concerning the protection of occupational health and safety. For the purposes of the implementation of the Model, it is necessary to consider that:

- the observance of the minimum safety standards laid down by specific sector regulations does not complete the required obligation of due diligence;

- it is necessary to ensure the adoption of security standards such as to minimise (and, if possible, eliminate) all risks of industrial accident and occupational disease, even under the best-known technique and science, depending on the nature of the work;
- the behaviour of the injured worker that caused the event does not exclude any liability on the part of the entity, when the event is however due to the lack or inadequacy of the precautions that, if adopted, would have counteracted the underlying risk of such behaviour. Liability is excluded only in the presence of the worker's behaviour that is exceptional, abnormal and excessive compared to the working process, organisational directives received and common prudence.

From the point of view of protected subjects, accident-prevention regulations do not protect only the Employees, but all the persons who lawfully enter the premises used for carrying out the work.

As regards active subjects, those who, by reason of their task, carry out Sensitive Activity on the matter, can commit these types of offences. For example:

- the worker who, through his/her own actions and or omissions, can compromise his/her own and others' health and safety;
- the manager and the person in charge, who can be liable, among other things, for coordinating and supervising training and information activities;
- the employer as the main actor in the field of prevention and protection.

G.2 Sensitive Activity

G.2.1. Introduction

In order to define Sensitive Activity in advance, it is necessary to consider, in accordance with the Decree, the activities within which industrial accidents can occur and those within which the offence for negligent violation of the regulations and of the existing prevention measures on the protection of health and safety at work can be committed by members of the organisation. To this end, the Company considered it strategic to draw inspiration from two important control and management tools:

- the risk assessment required by current regulations on health and safety protection;
- the BS OHSAS 18001:2007 Standard.

Risk assessment has been used to identify the conditions under which, reasonably, harmful events may occur.

The effective adoption of a health and safety at work management system implemented in accordance with the BS OHSAS 18001:2007 standard is recognised by the legislator, in those parts where it may be applicable, as a way to achieve the objectives of proper management of health and safety at work; therefore, as envisaged by Article 30 of Italian Legislative Decree 81/2008, an organisational model created in accordance with this rule would presumably comply with the exemptions provided for by the Decree.

Therefore, the Company drew its inspiration from the BS OHSAS 18001:2007 standard with the aim of controlling its activities, checking that they are, from the point of view of health and safety protection, in compliance with the provisions of local, national and European laws, rules and regulations and organising the entire management structure as a whole.

G.2.2. Sensitive Activity

The Sensitive Activity identified with reference to the offences mentioned by Article 25-septies of Italian Legislative Decree no. 231/2001 are broken down as follows:

- activities at risk of industrial accident and occupational disease, borrowed from the company's risk assessment document ("RAD") pursuant to Article 28 of Italian Legislative Decree no. 81 of 9 April 2008, drawn up by the employer and understood as activities where industrial accidents and occupational diseases can potentially materialise;
- activities at risk of offence, understood as the activities that may potentially give rise to the offences referred to in Article 25-septies of the Decree, in that their omission or ineffective implementation could constitute negligent liability, and which constitute the central element for adopting and effectively implementing a system suitable for the fulfilment of all the legal obligations required by the regulations in force on health and

safety at work. The Company, through an activity of control and risk assessment, which is an integral part of the Model, identified the activities at risk of offence and considered a possible deviation from their management system.

Activities at risk of industrial accident and occupational disease

Through careful investigations involving both structural and organisational aspects, risks to the safety and health of workers are identified.

The results of these investigations, which allow the identification of the risks that may give rise to industrial accidents and occupational diseases, are contained in the specific risk assessment documents that also indicate the protective measures for their elimination or containment. The activities within which industrial accidents or occupational disease may occur are therefore taken from the specific risk assessment documents to which this report refers.

The risk assessment documents are constantly updated with regard to new and potential prevention requirements, in accordance with the procedures envisaged by this Model.

Based on the results from the risk assessment carried out and in the light of the controls currently in place, the principles of behaviour and prevention protocols were identified (paragraphs 3 et seq. of this Section) that must be implemented to prevent, as far as reasonably possible and in accordance with the degree of development of science and technology, the omission or insufficient effectiveness of the measures taken to protect safety and health at work from which the criminal offences described above could derive.

Activities at risk of offence

The activities that may potentially give rise to the offences referred to in Article 25-septies of the Decree, in that their omission or ineffective implementation could constitute negligent liability on the part of the Company, are listed below. They were identified in accordance with the provisions of Article 30 of Italian Legislative Decree no. 81 of 9 April 2008 and by taking into account the requirements of the BS OHSAS 18001:2007 Standard on which the Model is based:

- identification of the applicable regulatory provisions to be complied with in order to comply with the technical and structural standards;
- definition of resources, roles and responsibilities to ensure activities aimed at the implementation of procedures and instructions for safe work by workers;
- risk assessment and preparation of the ensuing prevention and protection measures;
- identification and management of collective and/or individual protection measures to contain or eliminate risks;
- emergency management and management of firefighting and first aid activities;
- management of contracts;
- operating procedures and instructions for controlling particular risks;
- health surveillance activities;
- workers' expertise, information, training and awareness;
- controls on purchases, acquisition of documents and certifications required by law;
- maintenance activities aimed at meeting the applicable technical and health and safety standards;
- communication, participation and consultation activities, management of regular safety meetings, consultation of workers' safety representatives;
- management of documents and registration systems in order to ensure the traceability of activities.

The list of Sensitive Activity is periodically updated in relation to new and potential prevention requirements in accordance with the procedures envisaged by the Model.

G.3. General rules of conduct

The Model is not intended to replace the prerogatives and responsibilities of the law regulated by the subjects identified by Italian Legislative Decree no. 81 of 9 April 2008 and by the regulations further applicable in these cases. On the other hand, it is a further control measure and verification of the existence, effectiveness and adequacy of the structure and organisation carried out in compliance with the special regulations in force on accident

prevention and protection of safety and health at work.

All the exposed individuals under the Model, as identified in paragraph 4.4 of the General Part, adopt rules of behaviour in compliance with the principles contained in the Code of Ethics of the Company, in accident-prevention regulations as well as in the Model implementation instruments in order to prevent the occurrence of the crimes of culpable homicide and harm envisaged above.

In particular, the principles of behaviour identified in the Code of Ethics that is intended to be fully referred to herein and the documentation relating to protection and safety at work (including the RAD as well as the emergency management procedures) through which situations where it is reasonably possible that harmful events related to the work activity occur are identified, constitute a prerequisite and an integral part of the prevention protocols. The essential prerequisites of the Model for the prevention of accidents at work consists in the observance of certain principles and in certain behaviours of the workers of the Company, as well as by any external subjects who are lawfully at the premises of the Company. In particular, each worker and each subject who is lawfully at the premises of the Company, or whose activity falls under the responsibility of the Company, must:

- in accordance with their training and experience, as well as with the instructions and means supplied or prepared by the employer, not adopt an imprudent behaviour with regard to the protection of their own health and safety;
- comply with Group regulations and procedures for collective and individual protection, by carrying out in particular any adequate monitoring and activities appropriate to protect the health and safety of Suppliers and/or persons from outside the company, possibly present at the workplace;
- properly use the machinery, equipment, tools, dangerous substances and preparations, means of transport and other work equipment as well as safety devices;
- make appropriate use of the protection devices made available;

- immediately report to the person in charge (because of the assigned responsibilities) the anomalies of the means and devices mentioned above, as well as any other dangerous conditions of which they become aware;
- intervene directly, in the face of a danger observed and only in the cases of emergency, in accordance with their competences and possibilities;
- undergo the required health controls;
- undergo the required training;
- contribute to the fulfilment of all obligations imposed by the competent authority or however necessary to protect the workers' safety and health at work.

For these purposes, it is not allowed to:

- remove or modify without authorisation the safety or reporting or control devices;
- carry out on their own initiative transactions or operations not of direct concern or that may compromise their safety or that of other workers. Specific prevention protocols

G.4. Specific prevention protocols

The RAD indicates specific measures for the prevention of industrial accidents and occupational disease; with regard to these aspects, reference is made in full to that report.

As for the prevention measures for activities at risk of offence as identified above, i.e. the behaviour that could therefore integrate the liability of the Company in relation to accidents at work, this model of organisation, management and control is adopted and implemented in order to ensure the fulfilment of all relevant legal obligations.

For the purposes of adopting and implementing the Model, the principles and protocols indicated below apply.

Identification of the applicable regulatory provisions to be complied with in order to comply with the technical and structural standards

Compliance with regulations in force on the matter (laws, technical standards and regulations, etc.) is ensured through the adoption of specific records in order to put under control:

- identification and accessibility to regulations on the subject applicable to the organisation;
- legislative updating;
- regular monitoring of compliance with applicable laws and regulation.

Definition of resources, roles and responsibilities to ensure activities aimed at the implementation of procedures and instructions for safe work by workers

Technical and professional requirements - which may originate from specific regulatory provisions - are defined for all the figures identified for handling issues related to health and safety at work; the subjects have these requirements prior to the assignment of the task and can also be achieved through specific training; they must be maintained over time.

The assignment of specific responsibilities takes place in writing with certified date, setting out, in detail, characteristics and limits of the task and, if necessary, identifying the spending power.

In general, by way of example, through the procedures defined in the procedure:

- the responsibilities of management, coordination and control within the Company are formalised;
- the subjects envisaged by the regulations on hygiene and safety at the workplace (including, in the case of sites, the subjects envisaged by title IV, Italian Legislative Decree no. 81 of 9 April 2008) are properly designated and vested with the powers necessary to perform the role assigned to them;
- the system of delegations, powers of signature and spending powers is consistent with the responsibilities assigned;
- the assignment and exercise of powers under a decision-making process is consistent with positions of responsibility and with the relevance and/or criticality of the underlying risk situations;
- there is no subjective identity between those who take or carry out decisions and those who are required to carry out the controls envisaged by law and procedures covered by the supervisory system;

- the subjects in charge and/or appointed under the existing legislation on hygiene and safety at work have adequate and effective skills in this area.

Risk assessment and preparation of the ensuing prevention and protection measures

Since risk assessment is the key requirement for guaranteeing occupational health and safety and since it is the main tool for identifying measures of protection, be they the reduction or elimination of risk, risk identification and detection must be correctly carried out in compliance with the principle of truthfulness, completeness and accuracy. According to the binding legislation, this task is entrusted to the employer that relies on the support of other subjects such as the Prevention and Protection Service Manager and the occupational health specialist and after consulting the workers' safety representative.

All data and information used for risk assessment and consequently for identifying the measures of protection (e.g. technical documentation, instrumental measures, outcomes of internal surveys, etc.) must be clear, complete and truthfully represent the State of the art of the Company.

Data and information are collected and processed in a timely manner, under the supervision of the Employer, also by means of subjects identified by the Employer having appropriate qualifications - certifiable when required - of technical and, where appropriate, instrumental competence. On request, any document and source from which the information comes should be transmitted along with data and information.

The preparation of the RAD and the plan of prevention and protection measures is a task that cannot be delegated by the employer and must be carried out on the basis of the criteria defined in advance, in compliance with the provisions of Article 28 of Italian Legislative Decree no. 81 of 9 April 2008. These criteria forming an integral part of such documents envisage, among other things, the following aspects:

- routine and non-routine activities;
- activities of all persons who have access to the workplace (including external workers);
- human behaviour
- dangers from the outside;

- dangers related to working or created in the surrounding environment;
- infrastructures, equipment and material that are present at the workplace;
- changes to processes and/or the management system, including temporary changes and their impact on operations, processes and activities;
- any legal obligation applicable in the field of risk assessment and implementation of the necessary control measures;
- planning of working environments, machinery and plants;
- working and operating procedures.

Identification and management of collective and/or individual protection measures to contain or eliminate risks

As a result of the risk assessment carried out both at the time of preparation of the RAD and during preparation of the operational safety plans, in order to mitigate the risks, the necessary individual and collective safeguards to protect the worker are identified. The risk assessment process regulates:

- the identification of activities for which the use of personal protective equipment (“PPE”) is required;
- the definition of criteria for the choice of PPE, which must ensure the adequacy of PPE to the types of risk identified in the assessment phase and their compliance with current technical standards (e.g. CE marking);
- the definition of the method of delivery and storage of PPEs;
- the definition of a possible schedule of due dates to ensure the maintenance of protection requirements.

Emergency management and management of firefighting and first aid activities

Emergency management is implemented through specific plans that envisage:

- the identification of situations that can cause a potential emergency;
- the definition of methods responding to emergency conditions and preventing or mitigating their negative consequences on health and safety;
- the planning of the verification of the effectiveness of emergency management plans;

- the updating of emergency procedures in case of accidents or of negative results of periodical simulations.

Specific emergency management plans are defined. These plans are used to identify the exit paths and the methods used by employees with an employment contract to implement the measures for reporting and managing emergencies.

Employees with a subordinate employment contract include emergency workers; they are in a sufficient number and are previously trained in accordance with legal requirements.

Suitable fire-fighting systems chosen in type and number are available and maintained on the basis of the specific assessment of the risk of fire or of the information supplied by the competent authority; eligible healthcare measures are also present and maintained appropriate.

The effectiveness of the plans is guaranteed through periodic testing activities, aimed at ensuring that the personnel are fully aware of the correct behavioural measures and the adoption of appropriate recording tools to give evidence of the results of such tests and of the verification and maintenance activities of the controls prepared.

Management of contracts

Contract works and services are regulated by Article 26 of Italian Legislative Decree no. 81 of 9 April 2008.

The subject carrying out the works must have appropriate technical and professional requirements, verified also by the registration with the Chamber of Commerce, Industry, Crafts and Agriculture and self-certification of possession of the requirements. It must show compliance with the insurance and social security obligations towards its own personnel, also by submitting the Single contributory compliance document. If necessary, the contractor must also submit to INAIL a special declaration for any total or partial change to the activity already insured (on the basis of the type of intervention required and of the information supplied by the company).

The contractor, in the cases established by law, at the end of the interventions must issue the Declaration of conformity to the acknowledged rules of technology.

Operating procedures and instructions for controlling particular risks

Workplaces are designed also in compliance with the principles of ergonomics, comfort and wellbeing; defects that may affect workers' health and safety are regularly maintained to be eliminated as soon as possible. Appropriate hygienic conditions are ensured.

Any specific risk areas are appropriately reported and, where appropriate, made available only to subjects properly trained and protected.

Due to the complexity of the work, in particular with reference to the activities carried out at the sites, specific work instructions or operating procedures are envisaged that, together with the documentation concerning the methods of use of machinery and equipment and the safety documentation of the substances, are made accessible to the worker and are referred to in the safety operating plans, prepared for specific interventions.

Health surveillance activities

Prior to the assignment of any task to workers, it is necessary to verify the requirements both with regard to technical aspects (see subsequent Sensitive Activity: workers' expertise, information, training and awareness), and with regard to health aspects, whether satisfied in the risk assessment.

The fitness for work is verified by the occupational health specialist who, on the basis of the indications provided by the employer and of his/her knowledge of the workplaces and works, checks beforehand the fitness in terms of health of the worker by issuing opinions on the total or partial fitness, or unfitness for the task. Depending on the type of work required and of the results of the medical check, the occupational health specialist defines a health surveillance protocol to which the worker is subject.

Workers' expertise, information, training and awareness

All Employees receive appropriate information on the correct way to carry out their tasks and in the cases provided for by law, they are trained. This training must be supported with documentary evidence. Training activities are provided in different ways (e.g. classroom training, e-learning, written memos etc.) defined both by the choices of the Company and according to the provisions of the regulations in force.

The choice of the training subject can be bound by specific regulatory provisions.

In all cases, information, training and education activities are documented; the documents concerning personnel training are recorded and also used for the purpose of assigning new tasks.

Training will be carried out to:

- ensure, also through a proper planning, that any person under the control of the organisation is qualified on the basis of appropriate education, training or experience;
- identify the training needs related to the carrying-out of the activities and provide training or consider other actions to meet these requirements;
- assess the effectiveness of training or any other action implemented, and keep their records;
- ensure that the Employees become aware about the actual or potential impact of their work, the correct behaviour to adopt; their roles and responsibilities;

Controls on purchases, acquisition of documents and certifications required by law

The purchase of company equipment is carried out in compliance with their health and safety requirements taking also into account the workers' comments through their representatives. Equipment must comply with the regulations in force (e.g. CE marking, possession of a declaration of conformity issued by the installer, etc.). Where appropriate, on the basis of applicable law provisions, their commissioning will be subject to initial examination or approval procedures.

Prior to the use of new equipment, the worker in charge must be adequately trained.

Purchasing activities are carried out in accordance with the Group Purchasing Procedure with the aim of:

- defining the criteria and methods for qualifying and verifying suppliers' requirements;
- defining the methods for checking the compliance of the equipment to be purchased with the regulations in force (e.g. CE marking), as well as the methods and procedures for assessing the acceptability requirements;

- envisaging, where applicable, the methods for carrying out controls upon acceptance of initial examinations and approvals necessary for commissioning.

Maintenance activities aimed at meeting the applicable technical and health and safety standards

All equipment, machinery and plants that are likely to have significant impacts on health and safety are subject to planned maintenance protocols with timing and methods also defined by the manufacturers. Any specialised intervention is carried out by subjects meeting law requirements who will have to produce the necessary documents.

Maintenance activities on safety devices are recorded.

In the presence of equipment and plants for which the applicable legislation lays down a regular monitoring that is carried out by specific external entities (e.g. Regional Agency for environmental protection, Local Health Centres, Notified Bodies, Inspection Bodies etc.), a specific inspection contract will be signed with the entity in charge; if the entity in charge does not provide the service with the timing laid down by the legislation, the following will be carried out:

- should there be other subjects having the qualifications/permissions to carry out the monitoring, the task will be entrusted to them;
- in the absence of alternative subjects, the monitoring will be carried out, by way of self-diagnosis, through technical structures existing on the market (e.g. maintenance companies, engineering companies etc.).

Maintenance activities are managed through specific procedures with the aim of:

- defining the methods, timing and responsibilities for planning and carrying out maintenance and period checks, where required, of equipment, plants and machinery (accurately identified in specific protocols/cards) and the regular monitoring of their efficiency;
- defining the methods for recording maintenance operations carried out and related responsibilities;

- defining the methods for reporting anomalies, identifying the most suitable means for communicating such methods, identifying the subjects required to enable the process of maintenance (unplanned maintenance).

Communication, participation and consultation activities, management of regular safety meetings, consultation of workers' safety representatives

The procedures governing the involvement and consultation of personnel define the procedures for:

- internal communication between the various levels and structures of the organisation;
- communication with suppliers and other visitors at the workplace;
- receiving and responding to communications from external interested parties;
- employee participation, also by means of workers' representation, through:
 - their involvement in the identification of hazards, risk assessment and definition of the measures of protection;
 - their involvement in investigating an accident;
 - their consultation when there are changes that may have a significant impact on health and safety.

Management of documents and registration systems in order to ensure the traceability of activities

Document management is an essential requirement for maintaining the organisational and management model; through a correct management of the documents and the adoption of appropriate registration systems, the objective is to give evidence of what has been implemented, also ensuring the traceability of the decision-making process. It is also important to ensure the availability and updating of internal and external documents (e.g. documents relating to products and substances).

G.5. Additional checks

In specific implementation of the provisions of Article 18, paragraph 3-bis, Italian Legislative Decree no. 81 of 9 April 2008, regarding the supervisory duties of the employer and managers

on the fulfilment of obligations relating to safety in the workplace by persons in charge, workers, designers, manufacturers and suppliers, installers and occupational health specialist, the following specific protocols are envisaged.

Supervisory duties on the persons in charge (Article 19, Italian Legislative Decree no. 81 of 9 April 2008)

With particular reference to the supervision of the persons in charge, the Company implements specific protocols that require the employer, or person delegated by the employer:

- to programme and carry out spot-checks on the actual instruction received by subjects who access areas that expose them to a serious and specific risk;
- to programme and carry out spot-checks on the reports of anomalies by the persons in charge, as well as on the reports of anomalies relating to the behaviour of the persons in charge;
- to carry out checks on the reports of the persons in charge in relation to anomalies on work equipment and means of personal protection and other situations of danger, verifying the actions taken by the safety manager in charge and any follow up after the actions taken;
- to carry out checks on the actual use by the persons in charge of the internal training provided for this purpose.

Supervisory duties on the workers (Article 20, Italian Legislative Decree no. 81 of 9 April 2008)

With a special reference to the supervision of in-house workers, the Company implements specific protocols that require the employer, or person delegated by the employer:

- to programme and carry out spot-checks on the actual instruction received by the workers who access areas that expose them to a serious and specific risk;
- to programme and carry out spot-checks on the reports of anomalies by the persons in charge; to carry out checks on the actual use by the workers of the internal training provided for this purpose;

- to carry out checks on the actual use by the workers of the internal training provided for this purpose;
- to carry out checks on the actual submission of workers to health checks envisaged by law or in any case prepared by the occupational health specialist.

With a special reference to the supervision of the external workers, the Company implements protocols envisaged for the supervisory duties on designers, manufacturers, suppliers, installers and external maintenance men.

Supervisory duties on designers, manufacturers, suppliers, installers and external maintenance men and **contractors**

With particular reference to designers, manufacturers, suppliers, installers and external maintenance men of machinery, plant and any type of safety measure and work equipment, the Company implements specific protocols that envisage that:

- the scope of intervention and its impacts must be clearly defined in a written contract;
- accesses and activities on the site must be defined by third parties, with specific assessment of the risks related to their presence and related preparation of an information document on risks, signed by all external subjects involved and promptly adjusted in case of changes in the assumptions of the intervention;
- on delivery of machinery, plants and any type of safety equipment, the presence of CE markings, user and maintenance booklets, certificates of conformity and, if required, the homologation requirements, as well as the correspondence of product specifications with the requirements must be checked;
- contractual clauses regarding any non-compliance of third-party employees at company sites with regard to issues relating to safety in the workplace that envisage the activation of special reports and the application of penalties must be provided for;
- the supplier checking procedures must also take into account their compliance and the compliance of employees with safety procedures;
- the control by managers and the employer of compliance with the protocols listed above must be formalised and traceable.

With a special reference to the contractors, the Company implements specific protocols that require the employer, or person delegated by the employer, to prepare, in case of interferences, the Interference Risk Assessment Document (“DUVRI”, documento unico di valutazione dei rischi da interferenza). The DUVRI must be enclosed with the work contract. Supervisory duties on the occupational health specialist (Article 25, Italian Legislative Decree no. 81 of 9 April 2008)

With a special reference to the supervision on occupational health specialist, the Company implements specific protocols that require the employer:

- to check the possession by the occupational health specialist of the qualifications and requirements required by law for the performance of this function;
- to check that the occupational health specialist regularly attends coordination meetings with the Prevention and Protection Service Manager, the workers' safety representatives and the employer itself, dealing with issues of safety in the workplace, including those relating to corporate risk assessments and those with an impact on corporate social responsibility;
- to verify the correct and constant implementation by the occupational health specialist of the health protocols and company processes relating to health surveillance.

Additional specific checks

In accordance with the Model, further specific checks are set up to ensure that the organisational system of the Company, established in accordance with the applicable regulations on safety at work and accident prevention, is constantly monitored and placed in the best possible operating conditions.

For checking the effective implementation of the provisions of Italian Legislative Decree no. 81 of 9 April 2008 and the special regulations in force on accident prevention, protection of safety and health at the workplace:

- the persons qualified as employers, Prevention and Protection Service Manager and the occupational health specialist periodically bring the Supervisory Body of the Company up to date about issues relating to safety in the workplace;

- the delegated subjects envisaged by the regulations communicate without delay to the employer, or to the subject delegated by the latter, the deficiencies, anomalies and failures found;
- the Prevention and Protection Service Manager meets the Company's Supervisory Body on a regular basis in order to illustrate the most significant changes that are made to the RAD and to the procedures of the safety management system;
- the Employees, the Workers' Safety Representative, the occupational health specialist, the Prevention and Protection Service Manager and the employer can report to the Supervisory Body information and news on any deficiencies in the protection of health and safety in the workplace;
- the employer makes sure that all the subjects envisaged by the industry regulations are appointed, that they are provided with adequate, clear and sufficiently specific proxies, that they have the necessary skills and qualities, that they have powers, including spending powers, appropriate to the task and that the functions and proxies granted are effectively performed;
- in the performance of its functions, the Supervisory Body can request the assistance of the safety managers appointed by the Company, as well as of competent external consultants.

G.6. Audit activity for the periodic check of the application and effectiveness of the procedures of the specific prevention protocols

For the purposes of the control activities indicated above, specific audit activities are carried out by the QHSE Function, also with the collaboration of external consultants.

The audit activity is carried out by ensuring that:

- internal audits are carried out at planned intervals in order to determine whether the management system is correctly implemented and maintained in all its parts and is also effective in achieving the organisation's objectives;
- any deviations from the system are promptly managed;

- information on the results of the audits is transmitted to the employer, the Board of Directors and the Supervisory Body.

G.7. Implementation of specific prevention protocols

The specific prevention protocols listed above are applied in the management system of the procedures issued in accordance with the OHSAS 18001 standard and in the following relevant documents:

- P_STAFF01_GR “Employee Group Handbook – HR Procedure”;
- P_STAFF05.GR “Purchasing procedure”;
- P_STAFF07.GR “Procedure for managing Quality, Health, Safety, Environment (QHSE) activities”;
- P_FKRGRITA_N01_HR Procedure Management of company cars for mixed use Group - ITA”.

H. RECEIVING STOLEN GOODS, MONEY LAUNDERING AND USE OF MONEY, GOODS OR BENEFITS OF UNLAWFUL ORIGIN, AS WELL AS SELF-MONEY LAUNDERING (ARTICLE 25-OCTIES OF THE DECREE)

H.1 Applicable offences

Based on the analyses carried out, the following offences are considered as applicable to the Company:

- **receiving stolen goods**, envisaged by Article 648 of the Italian Criminal Code and identifiable whenever anyone, except for the cases of complicity in the offence, in order to obtain a profit for oneself or for others, purchases, receives and hides money or things coming from any crime or however, intervenes in purchasing, receiving or hiding them;
- **money laundering**, envisaged by Article 648-bis of the Italian Criminal Code and identifiable whenever anyone, except for the cases of complicity in the offence, replaces or transfers money, assets or other benefits coming from a non-negligent crime, i.e. it carries out in relation to them other operations in such a way as to obstruct the identification of their criminal origin;
- **use of money, goods or benefits of unlawful origin**, envisaged by Article 648-ter of the Italian Criminal Code and identifiable whenever anyone, except for the cases of complicity in the offence and the cases envisaged by Articles 648 and 648-bis, uses money, goods or other benefits from crime in economic or financial activities;
- **self-money laundering**, envisaged by Article 648-ter.1 of the Italian Criminal Code and identifiable whenever anyone, actually obstructing the identification of their criminal origin, uses, replaces or transfers the benefits coming from a non-negligent crime in economic or financial activities, or uses them with speculative purposes.

H.2. Sensitive Activity

The Company identified the Sensitive Activity that can be carried out in its own interest and/or in the interest of a subsidiary by virtue of specific intercompany contracts within the scope of which, potentially, some of the offences envisaged by Article 25-octies of the Decree could be committed:

- treasury, payments and funds management for the Company;
- management of intercompany relations;
- management of purchases of goods and services;
- management of corporate affairs and extraordinary transactions;
- tax management;
- activities to acquire/establish rights in areas owned by local/private bodies, to be allocated to the development/construction of energy production plants with renewable and non-renewable sources and expropriation procedures;
- plant design, construction and sale of created designs.

H.3. Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For transactions regarding **“Treasury, payments and funds management for the Company”**, the **“Management of intercompany relations”**, the **“Management of purchases of goods and services”**, the **“Management of corporate affairs and extraordinary transactions”** and **“Activities to acquire/ establish rights in areas owned by local/ private bodies, to be allocated to the development/ construction of energy production plants with renewable and non-renewable sources and expropriation procedures”**, the provisions of the prevention protocols and relevant procedures as per paragraph A.4 of this Special Part, with reference to the corresponding Sensitive Activity, shall apply.

For operations concerning “ **Tax Management**”, the provisions of the prevention protocols and relevant procedures referred to in paragraph D.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning “**Plant design, construction and sale of created designs**”, the protocols establish that:

- the activities must be carried out in coordination with the Business Development and M&A Division also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures required by the relevant applicable procedures;
- in the management of relations with current or potential customers, to which to sell the created designs, as well as in the negotiation phase, transparent relations must be maintained and no undue advantages, money or personal benefits may be offered to the representatives of investors / potential customers for negotiations to be successful (beyond customary courtesy and modest value limits);
- before commencing commercial relations with a counterparty, the appropriate checks must be carried out from an ethical and commercial perspective;
- potential new customers must also be evaluated in terms of reliability and ethics, by collecting information about: (i) subjective aspects of the counterparty and its representatives (for example, existence of criminal records, questionable reputation, admissions or statements by the counterparty regarding its involvement in criminal activities, counterparties using trust companies preventing the identification of the natural persons involved in the transaction); (ii) the conduct by the counterparty (for example ambiguous behaviour, lack of data necessary for carrying out transactions or reticence in supplying it); (iii) the corporate structure upstream of the customer; (iv) economic-financial aspects of the transaction (for example, unusual transactions based on type, frequency, timing, amount and geographical location); (v) the territorial spread

of the counterparty (for example, transactions carried out in “non- cooperative” countries);¹⁰

- all documents, requests and formal communications, which are intended for customers must be managed and signed only by previously identified and authorised persons;
- the traceability of the decision-making processes and the assessments carried out must be ensured, with reference to: (i) the possession of the expertise and resources necessary for the management of the contract, with respect to the activities requested by the customer; (ii) the powers and authorisations necessary to fulfil that ordered by the customer and any situations of conflict of interest; (iii) required clauses and guarantees;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- binding offers and contracts must be validated beforehand by formally identified Manager and signed by a party with appropriate delegated powers;
- the sale of created designs must be governed by a written contract clearing stating the price or the criteria for determining it;
- the contracts must be drafted, as possible, based on standards specified in agreement with the Legal & Corporate Affairs Unit or, alternatively, reviewed by the same;
- contracts governing relations with customer must include a specific clause: (i) requiring an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules

¹⁰ The lists may be consulted through the link on the website of Italy's Financial Intelligence Unit (FIU) in the section, "Home / Combating the financing of terrorism and the activities of countries that threaten international peace and security", or, alternatively, directly at:

- http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm, for the list prepared by the European Union;
- <http://www.treas.gov/offices/enforcement/ofac/sdn/>, for the OFAC (Office of Foreign Assets Control - United States Department of the Treasury) List;
- http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml, for the list prepared by the United Nations.

of conduct set forth in the Group's Code of Ethics; and (ii) stating the consequences in the event of a breach of that declared;

- the documentation produced, sent or received on the basis of the transaction must be properly filed in a specific archive by the Corporate Unit Managers involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_BUSLN01.GR Procedure for the management of Business Development and M&A activities”;
- P_BUSLN03.GR “Procedure for specifying and safeguarding Energy Management & Downstream Services activities”;
- P_STAFF04.GR “Procedure for managing legal activities”;
- P_STAFF16.GR “Administrative and accounting procedure for the management of the Sales Cycle”.
- P_BUSLN02.GR “Procedure for Engineering & Construction activities”;

H.4. Reporting of transactions/ operations considered potentially at risk in terms of “self-money laundering”

In addition to the above controls, the Corporate Units are required to monitor and report to the Supervisory Body the occurrence of the following transactions/operations considered potentially at risk in the “self-money laundering” area:

- payment of consultancy fees to companies located in “non-cooperative” countries 11;¹¹
- payments made for activities carried out by Italian counterparties but credited to current account of “non-cooperative” countries;
- increases in share capital carried out by companies based in “non-cooperative” countries;
- shareholders' loans from trust companies or trusts 12;¹²
- repeated transactions of a significant amount carried out with companies that have recently been created and have a general corporate purpose or are incompatible with the type of transaction in progress.

¹¹ The lists may be consulted through the link on the website of Italy's Financial Intelligence Unit (FIU) in the section, "Home / Combating the financing of terrorism and the activities of countries that threaten international peace and security", or, alternatively, directly at:

- http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm, for the list prepared by the European Union;
- <http://www.treas.gov/offices/enforcement/ofac/sdn/>, for the OFAC (Office of Foreign Assets Control - United States Department of the Treasury) List;
- http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml, for the list prepared by the United Nations.

¹² Identified according to the Italian Law 1966 of 23 November 1939 “Regulations of trusts and auditing companies”

I. CRIMES RELATING TO COPYRIGHT VIOLATION (ARTICLE 25-NOVIES OF THE DECREE)

I.1 Applicable offences

Based on the analyses carried out, the following crimes relating to copyright violation are considered applicable to the Company:

- **Article 171-bis, Italian Law no. 633 of 22 April 1941**, identifiable whenever anyone illegally duplicates, for profit, computer programmes or for the same purposes imports, distributes, sells, holds for commercial or entrepreneurial purposes or rents programmes on media not marked by the Italian Authors' and Publishers' Association (SIAE, Società italiana degli autori ed editori); uses any means intended to permit or facilitate the arbitrary removal or avoidance of software protections; for the purpose of making a profit, reproduces, transfers to other medium, distributes, communicates, presents or shows in public the contents of a database, extracts or re-uses the database, distributes, sells or rents a database on media that are not SIAE marked;
- **Article 171-ter, Italian Law no. 633 of 22 April 1941**, identifiable whenever anyone – among other things – illegally duplicates, reproduces, or disseminates in public literary, dramatic, scientific or educational, musical or musical-dramatic, multimedia works.

I.2 Sensitive Activity

The Company identified the Sensitive Activity that can be carried out in its own interest and/or in the interest of a subsidiary by virtue of specific intercompany contracts within which, potentially, some of the crimes relating to copyright violation envisaged by Article 25-novies of the Decree could be committed:

- management of IT systems;
- management of communication activities and use of copyrighted products (e.g. audio, video, content, etc.) for company activities (e.g. marketing, training, website, etc.);
- sales, marketing and business development management.

I.3. General principles of behaviour

All the **Model's Recipients** must ensure that the use of materials covered by intellectual property rights comply with legal and contractual provisions.

Within the scope of entering into contracts with service providers, a specific clause must be guaranteed which requires: (i) an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Company's Model (as applicable) and in the Group's Code of Ethics; (ii) stating the consequences in the event of a breach of that declared (including the termination of the contract).

Contracts with suppliers that support the Company within the scope of defining communication and marketing campaigns must provide adequate release from liability clauses for the Company with respect to any copyright infringement.

There is also an express prohibition on:

- infringing, for example by access to IT networks, rights on protected intellectual property or disseminating, in any way, intellectual property that is not meant for publication or seizing ownership;
- exploiting or disclosing printouts without the prior written authorisation by the owner of the intellectual property or the related economic exploitation rights;
- copy databases on mediums that are not marked by collective management bodies/independent management entities (for example SIAE), disclose, in any way, without the authorisation of the owner of the copyright or in breach of prohibitions imposed on the creator;
- remove or alter electronic information entered into protected works or appearing in their communications to the public, regarding the rights regime attached to them.

I.4 Specific prevention protocols and respective implementation

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For operations concerning the "**Management of IT systems**", the provisions of the prevention protocols and relevant procedures referred to in paragraph B.3 of this Special Part apply with reference to the corresponding Sensitive Activity (in particular "Hardware and Software Management").

For transactions regarding the "**Management of the communication activities and use of products protected by copyright (for example audio, video, content, etc.) for company activities (for example marketing, training, Internet sites, etc.)**", the provisions of the general principles of behaviour shall apply as set out in paragraph I.3 of this Special Part.

For operations concerning "**Sales, Marketing and Business Development Management**", the provisions of the prevention protocols and relevant procedures referred to in paragraph A.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

J. INCITEMENT NOT TO MAKE STATEMENTS OR TO MAKE FALSE STATEMENTS IN COURT (ART. 25-DECIES OF THE DECREE)

J.1. Applicable offence

Based on the conducted analyses, the following was considered as potentially applicable to the Company: the crime of incitement not to make statements or to make false statements in court envisaged by Article 377-bis of the Italian Criminal Code and identifiable whenever anyone, with violence or threat, or with offer or promise of money or other benefit, incites the person required to make before the court statements that can be used in criminal proceedings not to make statements or to make false statements in court, when this person has the right to silence.

J.2. Sensitive Activity

The circumstances referred to in art. 377-bis of the Italian Criminal Code, besides a generic connection to the “Management of disputes”, do not appear to be linked to specific business activities carried out by the Company, in addition to being covered by a specific system of controls, given that it could be committed at each company level and in an almost infinite number of ways.

J.3. Specific prevention protocols and respective implementation

The principles contained in the Code of Ethics constitute the most suitable tool for preventing the commission of the offence of incitement not to make statements or to make false statements in court.

Therefore, all the Exposed Individuals under the Model, in order to avoid a behaviour that may constitute this crime, adopt practices and behaviour that comply with the Code of Ethics; in particular, the recipients of the Model follow the ethical principles of the Company with regard to relations with the court and with subjects who, as part of judicial proceedings, are qualified as parties or witnesses.

K. ENVIRONMENTAL OFFENCES (ART. 25-UNDECIES OF THE DECREE)

K.1. Introduction

The introduction of environmental offences among the predicate offences of Italian Legislative Decree 231/2001, in force since August 2011, subsequently integrated with Law 68/15, gave the Company the impetus to start an investigation of the environmental management aspects relevant to the aforementioned offences, which led to the identification of the Sensitive Activity listed in paragraph K.3 below.

The prohibitions and general rules of behaviour and control set out in paragraph K.4 represent a first indication of the principles that all subject involved in such activities must follow in order to prevent the commission of the offences envisaged by the Decree and to ensure conditions of fairness and transparency in the carrying-out of environmental management activities, in line with the provisions of applicable laws and regulations.

For the purposes of this protocol, it is important to note that the Company adopts an integrated quality, safety and environmental management system that complies with the UNI EN ISO 14001 standard for environmental management. The adoption of this system helps to identify the applicable laws and regulations to the various “environmental matrices”, their observance, thanks to the identification of mandatory requirements, and the definition of codified and monitored procedures for compliance with these requirements.

K.2. Applicable offences

Based on the results of the investigation, the following is the list of offences pursuant to Article 25-undecies that the Company considers potentially applicable under normal operating conditions in the carrying-out of company activities.

- **Activities organised for the illicit trafficking of waste** as provided by Art. 452 quaterdecies of the Criminal Code and identifiable whenever anyone transfers, receives, transports, exports and imports, or in any case carries out the unauthorised management of large quantities of waste in order to obtain an unfair profit, with

several operations and through the setting-up of means and continuous organised activities;

- Violation of the requirements to notify, keeping of mandatory records and of forms, envisaged by Article 258, paragraph 4, second sentence, of Italian Legislative Decree no. 152 of 3 April 2006 and identifiable whenever anyone, in the preparation of a waste analysis certificate, provides false information on the nature, composition and chemical and physical characteristics of waste and uses a false certificate during transport.

K.3. Sensitive Activity

The Sensitive Activity identified with reference to the offences mentioned by Article 25-undecies of the Decree are broken down as follows:

- selection of suppliers of ordinary/extraordinary maintenance services and services for the disposal of waste produced by office activities and related activities for checking the requirements of OEM suppliers;
- obligations relating to the disposal of waste and related activities of compliance with regulatory requirements.

K.4. General rules of conduct

All Employees and Third Parties must:

- comply with the laws in force and the principles set out in this Model;
- comply with the obligations laid down by national and international standards on environmental protection and scrupulously observe the instructions given by the subjects in charge in order to preserve the environment;
- promptly report to the Corporate Units identified any situations of danger to the environment and violations of the rules of behaviour defined in this Model;
- operate in line with the existing system of delegation and powers;
- pursue the objective of “no harm to the environment”. Cost and time saving objectives must not be pursued at the expense of environmental protection.

Company Representatives specifically responsible for environmental compliance must also:

- define appropriate regulations, also identifying specific precautionary rules to be followed in order to ensure the environmental protection required;
- promote a culture in which all Employees and Third Parties participate in this commitment;
- guarantee, also through the formalisation of specific information, an adequate level of information to Employees, as well as to the workers of subcontractors and cooperatives, on the consequences deriving from a failure to comply with the law and the rules of behaviour and control defined by the Company itself;
- promptly report to the Corporate Units identified in accordance with the law and/or internally any reports/risk events/danger to the environment regardless of their seriousness.

It is also prohibited to adopt a behaviour that could constitute an offence included among those considered by Decree 152/06 (“Environmental Code”).

K.5. Specific prevention protocols

Introduction

The Company operates in accordance with an integrated management system (“IMS”) structured, as regards environmental management, according to the UNI ISO 14001 standard, as formalised in the IMS Manual, which is the first level document for the management of environmental risks, and which refers to operating and management procedures applied to all operational activities of the company. The IMS is configured as the general control unit to be observed by all Exposed Individuals and is supplemented by the operating procedures and by this protocol in order to complete the controls and the resulting fulfilments. The responsibility for coordinating the implementation of the IMS is entrusted to the IMS Manager, appointed by the Company, who is responsible for assessing and maintaining regulatory compliance, and is therefore the main management and organisational control unit.

The Company adopted a procedure (P005FKR “Identification, application and monitoring of legal and other requirements”) that defines the methods for identifying and accessing the applicable laws and regulations and assessing its specific requirements. A “Register of applicable laws” (D005_1FKR) is also available, which shows the state of compliance of the various company sites with environmental issues and the related deadlines (e.g. authorisations).

The assessment of environmental aspects and related significant risks is formalised in a procedure (P002FKR “Identification and assessment of environmental aspects”) that describes the methodology used to identify the environmental aspects/impacts of the activities carried out, the environmental risk related to them, the ways in which the latter are controlled and the procedures for on-going improvement. The results of the evaluations carried out are documented in the “Register of direct and indirect environmental aspects” (D002_2FKR). Moreover, the activity is kept under control by using the document “Environmental Schedule” (D005_4FKR) defining the periodicity and responsibility in maintenance/control operations.

Procedures are also in place for the Planning and implementation of training, information, awareness raising and internal communication activities both internally (which are carried out in agreement with the provisions of the procedure “P009FKR Information, training and education activities for Group personnel”) and towards interested parties (“P010FKR Internal and external communication, consultation and participation”).

With specific reference to the activities at risk identified pursuant to Article 25-undecies of Italian Legislative Decree 231/2001; note that these are carried out in compliance with the rules indicated in the procedure “P011FKR Waste Management”.

Specific control principles

The following are the principles of behaviour and related specific control measures applicable to normal operating conditions, compliance with which must be ensured.

For operations concerning the selection of **suppliers of ordinary/extraordinary maintenance services and services for the disposal of waste produced by office activities**, the protocols specify that:

- the selection of suppliers must be made in compliance with the provisions of protocol “A - Offences committed in relations with the Public Administration” of this Model and the related Group operating procedures; in particular when selecting suppliers:
 - the Company must check the existence of requirements pursuant to the law of the suppliers, acquiring a certified paper copy of the relative documentation where it is not possible to obtain the original copy;
 - the Company carries out periodic checks on the maintenance over time of the requirements pursuant to the law verified during the selection phase;
- the QHSE company Function monitors that third-party companies:
 - collect on site urban and similar waste and special waste in compliance with good technical and environmental prevention regulations and practices (for example, by separating waste by CER code and placing labels on containers), classifying it correctly and characterising it in the envisaged categories and classes of danger;
 - entrust urban and similar waste to ad hoc services authorised at local level by means of an appropriate convention for transport and disposal within the terms of the law, acquiring and maintaining the agreements of reference;
 - entrust special and hazardous waste and waste not deriving from maintenance activities to authorised transport, recovery and disposal companies registered with the relevant registers, making sure that the required authorisations, registrations or communications have been obtained, including from suppliers and consultants, and that copies have been acquired;
 - if subcontractors are used, they must be provided with appropriate authorisations.

With reference to the **requirements relating to waste disposal**, the protocols specify that the QHSE company Function must supervise the possible characterisation of waste produced

by the Company, using accredited third party laboratories and ensuring the truthfulness and completeness of the relevant declarations, must prepare and store the list of waste produced and the waste identification forms.

The Person in charge of the check/supervision activities described in the context of the specific prevention protocols has the task of filing/preparing the traceability of all the documentation produced as part of the described checks.

K.6. Audit activity for the periodic check of the application of the specific prevention protocols

For the purposes of the control activities indicated above, specific audit activities can be carried out by the QHSE company Function, also with the collaboration of external consultants.

The audit activity is carried out by ensuring that:

- internal audits are carried out at planned intervals in order to determine whether the management system is correctly implemented and maintained in all its parts and is also effective in achieving the organisation's objectives;
- any deviations from the system are promptly managed;
- information on the results of the audits is transmitted to the employer, the Board of Directors and the Supervisory Body.

K.7. Implementation of specific prevention protocols

The specific prevention protocols listed above are applied in the management system of the procedures issued in accordance with the UNI EN ISO 14001 standard and, in particular, in the following procedures:

- P_BUSLN01.GR Procedure for the management of Business Development and M&A activities”;

- P_BUSLN03.GR “Procedure for specifying and safeguarding Energy Management & Downstream Services activities”;
- P_BUSLN02.GR “Procedure for Engineering & Construction activities”;
- P_STAFF04.GR “Procedure for managing legal activities”;
- P_STAFF05.GR “Purchasing procedure”;
- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”.

L. CORRUPTION IN THE PRIVATE SECTOR (INCLUDED AMONG THE CORPORATE OFFENCES REFERRED TO IN ARTICLE 25-TER OF THE DECREE)

L.1. Applicable offences

On the basis of analyses carried out, the following corporate crime is considered to be a corporate crime (in addition to those identified above in paragraph E. "Corporate Crimes" to which reference should be made): **corruption in the private sector**, envisaged by Article 2635 of the Italian Civil Code and identifiable whenever directors, general managers, executives in charge of preparing the company's accounting documents, auditors and liquidators or anyone, within the company's organisational framework, exercise managerial functions other than those of the aforesaid subjects, as well as subjects managed or supervised by them, who, through a third party or otherwise, request or receive for themselves or for others, undue money or other benefits, or accept the promise thereof, to perform or omit an act in violation of the obligations concerning their office or loyalty obligations. The offence also applies to anyone who, through a third party or otherwise, offers, promises or gives undue money or other benefits to the subjects indicated above.

The offence of **incitement to corruption in the private sector**, envisaged by the new Article 2635 bis of the Italian Civil Code paragraph 1 was also considered applicable and identifiable whenever anyone, with the aim of violating official duties or loyalty obligations, offers or promises undue money or other benefits to directors, general managers, executives in charge of preparing the company's accounting documents, auditors and liquidators or to those with managerial functions, should the offer or promise not be accepted.

L.2. Sensitive Activity

The Company identified the Sensitive and instrumental activities that can be carried out in its own interest and/or in the interest of a subsidiary by virtue of specific intra-group contracts within which, potentially, the offence of corruption in the private sector envisaged by Article

25-ter of the Decree (with specific reference to corruption in the private sector and/or the incitement to corruption in the private sector):

- treasury, payments and funds management for the Company;
- management of corporate affairs and extraordinary transactions;
- management of intercompany relations;
- personnel selection, recruitment, development;
- administrative management of personnel and reimbursement of expenses;
- management of capital goods and company benefits (e.g. cars, mobile phones, personal computers, corporate credit cards, etc.)
- management of gifts, gratuities, donations and sponsorships;
- management of purchases of goods and services;
- activities to acquire/establish rights in areas owned by local/private bodies, to be allocated to the development/construction of energy production plants with renewable and non-renewable sources and expropriation procedures;
- sales, marketing and business development management;
- Plant design, construction and sale of created designs;
- management of relations with Shareholders, the auditing company and the Management Control Committee

L.3 General rules of conduct

All the Company Representatives must promptly report the following to their immediate superiors: a) any attempts by representatives and/or employees of third-party counterparties with whom the Company has business relations to make undue requests, for example to obtain favours, unlawful money donations or other benefits; b) any critical issues or conflict of interest arising as part of relations with representatives and/or employees of third-party counterparties with whom the Company has business relations.

It is forbidden to pay or offer, directly or indirectly, even in various forms of aid and contributions, payments or material benefits to representatives and/or employees of third-

party counterparties with whom the Company has business relations or to persons close to them, in order to illegally influence their behaviour and ensure advantages of any kind to the Company.

L.4. Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For transactions regarding **“Treasury, payments and funds management for the Company”**, the **“Management of corporate affairs and extraordinary transactions”**, the **“Management of intercompany relations”**, the **“Recruitment, hiring and development of staff”**, the **“Administrative management of staff and reimbursement of expenses”**, the **“Management of operating assets and company assets (for example, cars, mobile phones, personal computers, company credit cards, etc.)”**, **“Management of presents, gifts, donations and sponsorships”**, the **“Management of purchases of goods and services”**, the **“Acquisition /establishment of rights in areas owned by local/private entities, to be allocated to the development/ construction of energy production plants with renewable and non-renewable sources and expropriation procedures”**, **“Sales, marketing and business development management”**, the provisions of the prevention protocols and relevant procedures as per paragraph A.4 of this Special Part, with reference to the corresponding Sensitive Activity, shall apply.

For operations concerning the **“Management of relations with Shareholders, the auditing firm and the Management Control Committee”**, the provisions of the prevention protocols and relevant procedures referred to in paragraph E.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning “ **Plant design, construction and sale of created designs**”, the provisions of the prevention protocols and relevant procedures referred to in paragraph H.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

M. EMPLOYMENT OF ILLEGALLY STAYING THIRD-COUNTRY NATIONALS (ARTICLE 25-DUODECIES OF THE DECREE)

M.1. Applicable offences

Based on the analyses carried out, the offence of employment of illegally staying third-country nationals (Article 22 of Italian Legislative Decree no. 286 of 25 July 1998), also understood as aiding and abetting the illegal stay of foreigners in the territory of the State (Article 25-duodecies par. 1-ter, introduced by Italian Law no. 161/2017 and included among the offences referred to in Article 25-duodecies of the Decree) is considered as potentially applicable to the Company and identifiable whenever the employer who employs foreign workers without residence permit or whose permit is revoked, cancelled or expired, and whose renewal has not been requested within the terms of the law.

M.2. Sensitive Activity

The Company identified the following Sensitive Activity, within which the offence of employment of illegally staying third-country nationals envisaged by Article 25-ter of the Decree could potentially be committed:

- personnel selection, recruitment, development;
- administrative management of personnel and reimbursement of expenses.

M.3. Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For operations concerning the "**Recruitment, hiring, development of staff**" and the "**Administrative management of staff and reimbursement of expenses**", the provisions of the prevention protocols and relevant procedures referred to in paragraph A.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

N. TAX CRIMES (ART. 25-QUINQUIESDECIES OF THE DECREE)

N. 1. Applicable offences

The introduction into Art. 25-quinquiesdecies of the Decree, tax crimes within the range of predicate offences, in accordance with Decree Law no. 124 of 26 October 2019, converted with Law no. 157 of 19 December 2019 and the subsequent Legislative Decree no. 75 of 14 July 2020 - encouraged the Company to start up an investigation into the relevant tax and duty management aspects with respect to said crimes, which led to the identification of the Sensitive Activity listed in paragraph No. 2 below.

Based on the analyses carried out, the following offences pursuant to art. 25-*quinquiesdecies* of the Decree, are considered as potentially applicable to the Company¹³:

- **Fraudulent statement through the use of invoices or other documents for non-existent transactions**, provided for under article 2, paragraph 1 and 2-bis of Legislative Decree 74/2000 and entailing behaviour by people, who, in order to evade income taxes or value added taxes, using invoices or other documents for non-existent transactions, indicates fake taxable persons in one of the statements relating to said taxes;

¹³ Law no. 157/2019 relating to the "Conversion into law, with amendments of Decree Law no. 124 of 26 October 2019, containing urgent provisions on tax matters and for requirements which cannot be postponed" provided for the addition to Legislative Decree 231/2001 of article 25-quinquiesdecies "Tax Crimes" and in particular, the crimes of "Fraudulent statement by the use of invoices or other documents for non-existent transactions" (article 2, paragraph 1 and 2-bis of Legislative Decree 74/2000), "Fraudulent statement using other devices" (article 3, Legislative Decree 74/2000), "Issue of invoices or other documents for non-existent transactions" (article 8, paragraph 1 and 2-bis of Legislative Decree 74/2000), "Hiding or destruction of accounting documents" (article 10, Legislative Decree 74/2000) and "Fraudulent failure to pay taxes". Subsequently, on 30 July 2020, Legislative Decree 75/2020 came into effect containing "Implementation of directive (EU) 2017/1371 relating to the fight against fraud that hurts the financial interests of the Union through criminal law", which introduced a number of amendments regarding the administrative responsibility of entities, including the addition to article 25-quinquiesdecies of the "Untruthful Statement" (article 4 Legislative Decree 74/2000), "Failure to make a statement" (article 5 Legislative Decree 74/2000) and "Improper payment" (article 10-quater Legislative Decree 74/2000) applicable upon the occurrence of three necessary conditions: i) the crime must have been committed within the scope of fraudulent cross-border systems; ii) the crime must have been committed in order to avoid value added tax; iii) the total amount of the evasion must not be less than €10 million.

- **Fraudulent statement by other deception**, provided under article 3 of Legislative Decree 74/2000 and entailing behaviour by persons who, in order to avoid income taxes or value added taxes, carry out objectively or subjectively fictitious transactions or uses false documents or other fraudulent means that could prevent the ascertainment and mislead the financial administration, indicates in one of the declarations relating to said taxes, related to said taxes, payable elements for an amount lower than the real amount or fake taxable persons or fictitious receivables or withholdings;
- **False tax statement** as provided for by article 4 of Legislative Decree 74/2000 and comprising conduct that, in order to avoid income taxes or value added taxes, indicates in one of the annual declarations relating to said taxes, payable elements for an amount that is less than the actual amount or non-existent payable elements;
- **Failure to make a statement** as provided under article 5 of Legislative Decree 74/2000 and entailing behaviour of persons who, in order to evade income tax or value added tax, do not submit, even though so obliged, one of the tax statements relating to said taxes;
- **Issuing invoices for non-existent transactions**, provided for under article 8 of Legislative Decree 74/2000 and entailing behaviour by persons who, in order to permit third parties to avoid income taxes or value added taxes, issues or releases invoices or other documents for non-existent transactions;
- **hide or destroy accounting documents**, as provided by article 10 of Legislative Decree 74/2000 and entailing behaviour by persons who, in order to evade income taxes or value added taxes, or to permit third parties to evade taxes, hides or destroys in whole or in part the accounting records or the documents that have to be kept, so that income or turnover cannot be reconstructed;
- **Undue compensation**, provided for under article 10-quarter of Legislative Decree 74/2000 entailing behaviour by persons who, when paying the amounts, use for

compensation, in accordance with article 17 of Legislative Decree no. 241 of 9 July 1997, receivables which are not due;

- **Fraudulent failure to pay taxes** provided for by article 11 of Legislative Decree 74/2000 and entailing behaviour by persons who, in order to avoid payment income taxes or value added taxes or interest or administrative sanctions relating to said taxes of a total amount of higher than € fifty thousand, fictitiously sells or carries out other fraudulent actions on its own or other goods that could make the enforced recovery invalid in whole or in part.

N. 2. Sensitive Activity

The Company identified the Sensitive Activity listed below, within which, potentially, the offences of crimes envisaged by Article 25 *quinquiesdecies* of the Decree could be potentially committed:

- management of purchases of goods and services;
- selection of suppliers of disposal services or any ordinary/extraordinary maintenance services;
- provision and management of fiduciary advice (of a legal, technical, notarial and tax nature);
- treasury, payments and funds management, as well as Public Administration-related credit management;
- management of the purchase of electricity from third parties in order to dispatch it on the energy market;
- management of corporate affairs and extraordinary transactions;
- management of disputes;
- management of intercompany relations;
- management of subsidised loans or other government funding;
- sales, marketing and business development management;
- management of gifts, gratuities, donations and sponsorship;

- bookkeeping, financial statements management and periodic reporting;
- management of capital goods and company benefits (e.g. cars, mobile phones, personal computers, corporate credit cards, etc.);
- management of IT systems;
- administrative management of personnel and reimbursement of expenses
- tax management;
- management of relations with the Public Administration, including, but not limited to, requests for opinions, authorisations, licences or authorisations for the acquisition / development / construction / operation of energy production plants with renewable and non-renewable sources, (ii) inspections, (iii) energy efficiency improvement for buildings and public roads including “smart” energy management;
- activities to acquire/establish rights in areas owned by local/private bodies, to be allocated to the development/construction of energy production plants with renewable and non-renewable sources;
- sale of measurement instruments and software and related services;
- provision of energy efficiency services;
- Plant design, construction and sale of created designs.

N. 3. General rules of conduct

The following is expressly prohibited for all **Recipients of the Model**:

- to use invoices or other documents for non-existent transactions and register them in the obligatory accounting records, indicating fictitious payable elements in one of the tax statements relating to income taxes or value added taxes;
- carry out objectively or subjectively fictitious transactions or uses false documents or other fraudulent means that could prevent the ascertainment and mislead the financial administration, indicates in one of the declarations relating to income taxes or value

added taxes, related to said taxes, receivable elements for an amount lower than the real amount or fictitious payable elements or fictitious receivables or withholdings;

- issue or release invoices or other documents for non-existent transactions in order to permit third parties to avoid income taxes or value added taxes;
- fail to submit one of the tax statements relating to the value added taxes where there is a specific regulatory requirement;
- use receivables which are not due or non-existent for offsetting purposes;
- hide or destroy in whole or in part the accounting records or documents that it is necessary to keep, in a way that income or business turnover cannot be reconstructed;
- fictitiously sell or carry out other fraudulent actions on its own or other assets that could make the enforced recovery invalid in whole or in part;
- indicate in the documentation, submitted for the purpose of the tax settlement procedure, assets for an amount lower than the real amount or fictitious payable elements.

N. 4. Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For transactions regarding **“Management of purchases of goods and services ”**, the **Assignment and management of fiduciary consultancies (legal, technical, notarial, tax”**, the **“Management of treasury, payments and financial resources”** and **"credit management with respect to the Public Administration"**, the **"Management of corporate affairs and extraordinary transactions"**, the **"Management of disputes"**, **"Management of intercompany relations"**, the **“Management of subsidised loans or other public loans”**, the **“Commercial, marketing and business development managements”**, **“Management of gifts,**

presents, donations and sponsorships " the "**Management of operating assets and company assets (for example cars, mobile phones, personal computers, company credit cards, etc.**", the "**Administrative management of staff and reimbursement of expenses**", the "**Management of relations with the Public Administration**" and the "**Activities of purchasing /establishment of rights on the areas of the owners of local/private entities to be used for the development/construction of energy production plants from renewable and non-renewable sources**", the provisions of the prevention protocols and relevant procedures as per paragraph A.4 of this Special Part, with reference to the corresponding Sensitive Activity, shall apply

For operations concerning "**IT management systems**", the provisions of the prevention protocols and relevant procedures referred to in paragraph B.3 of this Special Part apply with reference to the corresponding Sensitive Activities.

For operations concerning "**Bookkeeping, management of the financial statements and periodic reports**" and the "**Tax Management**", the provisions of the prevention protocols and relevant procedures referred to in paragraph D.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

In addition to the above-mentioned prevention protocols and procedures, in order to strengthen the control measures of the 'Tax Management' process, the Company has implemented a system for the detection, measurement, management and control of tax risk (the "**Tax Control Framework**" or "**TCF**").

For operations concerning "**Plant design, construction and sale of created designs**", the provisions of the prevention protocols and relevant procedures referred to in paragraph H.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

For the transactions regarding "**Selection of suppliers for services of disposal and any ordinary/extraordinary maintenance services**", the protocols provide that the selection of the suppliers has to be carried out in accordance with the provisions of protocol "A - Offences committed in relations with the Public Administration" of this Model, the operating procedures of the Group and the PSA Procedure PRI 011_7 TRZ - Management of Waste; more specifically, when selecting the suppliers:

- The Technical Director will indicate the technical characteristics needed for the service in the Purchasing Requests;
- Procurement and General Services will check, in coordination with the Technical Management, the existence of requirements pursuant to the law of the suppliers, acquiring a certified paper copy of the relative documentation where it is not possible to obtain the original copy;
- Procurement & General Services will carry out, in coordination with the Technical Management, periodic checks of the maintenance over time of the legal requirements verified at the selection stage.

The specific prevention protocols listed above are applied in the management system of the procedures issued in accordance with the UNI EN ISO 14001 standard and, in particular, in the following procedures:

- P_BUSLN01.GR Procedure for the management of Business Development and M&A activities.”;
- P_BUSLN02.GR “Procedure for Engineering & Construction activities”;
- P_STAFF04.GR “Procedure for managing legal activities”;
- P_STAFF05.GR “Purchasing procedure”;
- P_STAFF18.GR “Administrative and accounting procedure for managing fixed assets”
- P_BUSLN06.GR “Procedure for managing Thermal Generation activities”.

For transactions regarding the "**Management of the purchase of electricity from third parties in order to dispatch it on the energy market**", the protocols provide as follows:

- the entire process must be consistent with criteria of transparency and non-discrimination;
- all documentation relating to energy purchases must certify the method used and the procedure followed to make the purchase, the subject matter, the amount and the reasons underlying the choice of the supplier;
- there must be a separation of tasks between those who authorise, those who control and those who carry out the operations;
- the purchase of energy must be regulated by a written contract in which the price or the criteria for determining it is clearly set out;
- when choosing the suppliers, predefined subjective or objective criteria must be evaluated in advance, including the reputation and reliability of the subject on the market, as well as compliance with values common to those expressed in the Code of Ethics and in the Model of the Company;
- the invoices received by the Company relating to the purchase of energy must be recorded exclusively on the basis of suitable evidence that it has been purchased;
- the company Function Manager involved in the purchase must immediately inform the SB of any anomalies in the purchasing procedure or special requests made to the Company by this subject;
- the documents produced or received in connection with the purchase of energy must be properly kept by the Line/Division Function Managers in order to allow the correct traceability of the entire process and to facilitate any subsequent controls.

The specific prevention protocols listed above are applied in the following relevant documents:

- P_BUSLN03.GR "Procedure for managing Energy Management & Downstream Services activities";
- P_STAFF04.GR "Procedure for managing legal activities";

- P_STAFF16.GR “Administrative and accounting procedure for the management of the Sales Cycle”;
- I_STAFF12.GR “Operating instruction for the management of relations with the Public Administration”.

For transactions regarding the "**Sale of the measurement instruments and related software and services**" and "**Provision of services for energy efficiency**", the protocols provide as follows:

- the commercial activities must be carried out in coordination with the Energy Management Division and Downstream Services Division also by virtue of specific intercompany contracts and in compliance with the rules and operating procedures required by the relevant applicable procedures;
- in the management of current or potential customers, transparent relations must be maintained and no undue advantages, money or personal benefits may be offered to the representatives of the potential customers for negotiations to be successful (beyond customary courtesy and modest value limits);
- potential new customers must also be evaluated in terms of reliability and ethics, by collecting information about: (i) subjective aspects of the counterparty and its representatives (for example, existence of criminal records, questionable reputation, admissions or statements by the counterparty regarding its involvement in criminal activities, counterparties using trust companies preventing the identification of the natural persons involved in the transaction); (ii) the conduct by the counterparty (for example ambiguous behaviour, lack of data necessary for carrying out transactions or reticence in supplying it); (iii) the corporate structure upstream of the customer; (iv) economic-financial aspects of the transaction (for example, unusual transactions based on type, frequency, timing, amount and geographical location); (v) the territorial spread of the counterparty (for example, transactions carried out in “non- cooperative” countries);

- all documents, requests and formal communications, which are intended for customers must be managed and signed only by previously identified and authorised persons;
- the service is provided in accordance with the work environment, time-frames, results and levels of service agreed with the customer and recorded in the related contract;
- if the costs that emerge at the planning stage significantly exceed those hypothesised at the start of the project, the approving parties must be informed;
- the issue of the invoices must be requested on the basis of the invoicing plan provided and the state of progress of the activities;
- the contracts must be drafted based on standards specified in agreement with the Legal & Corporate Affairs Unit;
- contracts governing relations with customer must include a specific clause: (i) requiring an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Group's Code of Ethics; and (ii) stating the consequences in the event of a breach of that declared;
- the traceability of the decision-making processes and the assessments carried out must be ensured, with reference to: (i) the possession of the expertise and resources necessary for the management of the contract, with respect to the activities requested by the customer; (ii) the powers and authorisations necessary to fulfil that ordered by the customer and any situations of conflict of interest; (iii) required clauses and guarantees;
- the traceability and verifiability of the operations carried out must be guaranteed by storing the supporting documents;
- the company representatives involved must promptly report to the Supervisory Body any anomalous situations and critical issues found;

Further controls applicable if business agents/mediators are used

- the reputation, professionalism, expertise, independence and reliability of the party on the market, as well as the absence of conflicts of interest must be assessed in advance upon choosing a business promoter/broker;
- the service must be governed by a written agreement, clearly specifying the following: (i) the purpose, nature and timing of rendering the service, (ii) the structure of the fees, and (iii) the amount of the fees or the criteria for determining them;
- contracts with business promoters/brokers must be entered into exclusively by authorised subjects and in compliance with the system of powers in force;
- contracts governing relations with business promoters/brokers must include a specific clause: (i) requiring an express declaration by the counterparty that it is aware of and will comply with the provisions of Legislative Decree 231/2001 and that it agrees to comply with the rules of conduct set forth in the Group's Code of Ethics and, as applicable, in the Company's Model; (ii) stating the consequences in the event of a breach of that declared (including the termination of the contract itself).

The specific prevention protocols listed above are applied in the following relevant documents:

- P_BUSLN03.GR "Procedure for managing Energy Management & Downstream Services activities";
- P_STAFF04.GR "Procedure for managing legal activities";
- P_STAFF16.GR "Administrative and accounting procedure for the management of the Sales Cycle";
- I_STAFF12.GR "Operating instruction for the management of relations with the Public Administration".

O. OFFENCES RELATING TO NON-CASH PAYMENT INSTRUMENTS (ART. 25-OCTIES.1 OF THE DECREE);

O.1. Applicable offences

Legislative Decree 184/2021 introduced Offences relating to non-cash payment instruments into the range of offences provided for under the Decree, under article 25-*octies.1*, , which extends the catalogue of predicate offences to the following cases:

- **Undue use and falsification of non-cash payment instruments**, provided by article 493-*ter* of the criminal code and comprising behaviour by persons who, in the end obtain an advantage for themselves or others, unduly use, not being the owner, credit or payment cards, or any other similar document that enables the withdrawal of cash or the purchase of goods or the provision of services or in any case, any other non-cash payment instrument; it also includes those who, in order to obtain an advantage for themselves or for others, falsify or alter the instruments or documents described in the first sentence, or possess, transfer or purchase those instruments or documents of illegal provenance or in any case falsified or altered, and payment orders produced with them.
- **Holding and distributing devices, equipment or computer programmes aimed at committing offences regarding non-cash payment instruments** as provided under article 493-*quater* of the criminal code, and entailing the behaviour of persons who, in order to make use or permit others to use in the commission of offences regarding non-cash payment instruments, produce, import, export, sell, transport, distribute, make available or in any way obtain for themselves or others, devices, equipment or computer programmes that, due to the technical-construction or design characteristics, are mainly constructed to commit those offences or are specifically adapted for that reason.
- **IT fraud** provided by Article 640-*ter* of Italian Criminal Code and identifiable whenever anyone, by changing in any way the operation of an IT or telematic system or by

intervening in any way without any right on data, information or programmes contained in an IT or telematic system or pertaining to it, gets an unlawful profit for oneself or others.

O.2. Sensitive Activity

The Company identified the Sensitive Activity listed below, within which, potentially, the non-cash payment instrument offences envisaged by Article 25-*octies* of the Decree could be potentially committed:

- Treasury, payments and funds management, as well as Public Administration- related credit management;
- Administrative management of personnel and reimbursement of expenses;
- Management of capital goods and company benefits (e.g. cars, mobile phones, personal computers, corporate credit cards, etc.);
- Management of purchases of goods and services;
- Management of the purchase of electricity from third parties in order to dispatch it on the energy market;
- Management of IT systems;

O.3. Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For operations concerning the **"Management of the treasury, payments and financial resources and the management of credit to the Public Administration"** , the provisions of the prevention protocols referred to in paragraph A.4 of this Special Part apply, with reference to the corresponding Sensitive Activity.

For operations concerning **“Administrative management of personnel and reimbursement of expenses”**, the provisions of the prevention protocols and relevant procedures referred to in paragraph A.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning **"Management of capital goods and company benefits" (for example cars, mobile phones, personal computers company credit cards, etc.)** , the provisions of the prevention protocols referred to in paragraph A.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning **“Management of the purchase of goods and services”**, the provisions of the prevention protocols and relevant procedures referred to in paragraph A.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning **“Management of purchases of electricity from third parties in order to dispatch it onto the energy market”**, the provisions of the prevention protocols and relevant procedures referred to in paragraph N.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning the **“Management of IT systems”**, the provisions of the prevention protocols and relevant procedures referred to in paragraph B.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

P. CRIMES AGAINST CULTURAL HERITAGE (ARTS. 25-SEPTIESDECIES AND 25-DUODEVICIES OF THE DECREE).

P.1. Applicable offences

Law no. 22 of 9 March 2022 regarding the reform of crimes against cultural heritage introduced articles *25-septiesdecies* and *25-duodevicies* into the range of crimes provided for under the Decree. Based on the analyses carried out, the following offences pursuant to art. *25-septiesdecies* and *25-duodevicies* of the Decree are considered as potentially applicable to the Company:

- **Distribution, dispersion, deterioration, defacement, contamination and unlawful use of cultural or landscape assets** provided for under article 518-duodecies of the criminal code and comprising the behaviour of persons who destroy, disperse, deteriorate or make cultural or landscape assets or other assets unserviceable or unusable, or outside these cases, allocate cultural assets to a use that is incompatible with their historical or artistic character or damage their storage or completeness in the interest of or to the benefit of the Company.
- **Destruction and plundering of cultural or landscape assets**, provided for under article 518-terdecies of the criminal code comprises behaviour by persons who destroy or plunder assets relating to cultural or landscape assets or institutions or places of culture, in the interest of or to the benefit of the Company.

P.2. Sensitive Activity

The Company identified the Sensitive Activity listed below, within which, potentially, the offences of crimes against the cultural heritage envisaged by Article *25--septiesdecies* and *25-duodevicies* of the Decree could be potentially committed:

- Sales, marketing and business development management;
- Sale of the measurement instruments and related software and services; provision of services for energy efficiency;

- Design of systems of subsidiaries;
- Plant design, construction and sale of created designs.

P.3. Specific prevention protocols

This paragraph refers to the prevention protocols and the relevant procedures that must be followed by anyone who manages, coordinates and supervises the operations listed below, also under a service contract.

For operations concerning “**Sales, Marketing and Business Development Management**”, the provisions of the prevention protocols and relevant procedures referred to in paragraph A.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning the “**Sale of measurement instruments and connected software and services; provision of services for energy efficiency**”, the provisions of the prevention protocols and relevant procedures referred to in paragraph N.4 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning “**Plant design and construction of subsidiaries**”, the provisions of the prevention protocols and relevant procedures referred to in paragraph D.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

For operations concerning “**Plant design, construction and sale of created projects**”, the provisions of the prevention protocols and relevant procedures referred to in paragraph H.3 of this Special Part apply with reference to the corresponding Sensitive Activity.

In addition to the above-mentioned prevention protocols and procedures, in order to reinforce the control system, further controls have been provided for:

- the activity prior to issuing the authorisation to design the plants are subject to specific controls and monitored by the Manager of the company Unit involved in accordance with the operating procedures provided for by the applicable reference procedures;

- the technical documents to send to the public Entities involved are subject to the control of the applicable company Units and are reviewed and signed by the Legal representative of the company;
- the produced, sent and received documentation must be promptly filed by the Corporate Unit Manager involved in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- the work carried out is constantly monitored by the parties in charge and compliance with the applicable laws is guaranteed and any orders issued by the public Entities involved.