Modello di organizzazione e gestione ex D.Lgs. 8 giugno 2001, n. 231

Engineering D.HUB S.p.A.

Version approved by the Board of Directors on 17/03/2021

Written by:	Internal Audit Function
Checked by:	A. Quintavalle
Version no.:	5.0
No. of pages:	95
Distribution:	Company intranet website

File name: DHB_Modello_di_Organizzazione_e_Gestione_231_English_version 5.0

Warning

The original version of this document is available on the company network server.
All paper copies are considered to be **uncontrolled working copies**.
Those using uncontrolled copies are responsible for checking their update status.

VERSION UPDATES

Version	Date	Reason	Amendments
1.0	04/08/2014	New issue	New issue
2.0	08/03/2016	Comprehensive review	▪ Complete update due to inclusion by the Legislator of new crimes within the scope of application of Legislative Decree 231/01 ▪ Streamlining of the Model structure, with the inclusion of general and specific Principles of behavior by type of crime ▪ Increased the frequency of periodic information flows to the Supervisory Board
3.0	21/09/2017	▪ Comprehensive review in order to adapt to legislative developments ▪ Review due to delisting the shares of Engineering Ingegneria Informatica S.p.A. ▪ New organization chart of 16/06/2017	▪ Introduction of art. 603-*bis* of the Criminal Code, as amended by Law no. 199/2016 and included in art. 25-*quinquies* of Legislative Decree 231/01 ▪ Introduced the provision contained in art. 23 of Legislative Decree 231/01 ▪ Changes in the crime of Bribery between private parties ▪ Introducing the crime of instigating bribery between private parties ▪ Elimination of Special Sections of the Model that are no longer pertinent to the Company's reality following the delisting of the shares of Engineering Ingegneria Informatica S.p.A. on 8 July 2016 ▪ Updated §1.2.2

4.0	13/03/2019	▪ Update of the "Engineering Italia Group Organization Manual" ▪ Introduction of Law 179 dated 30 November 2017 on Whistleblowing ▪ Modification of art. 25-duodecies of Legislative Decree 231/01 ▪ New organization chart of 21/12/2018 (Prot. 03/2018 D-HUB/AD-FB/VA/lr)	▪ Update of the section dedicated to the description of the organizational structure of the Company ▪ Introduction of the section dedicated to Whistleblowing ▪ Revision of the section dedicated to the disciplinary system, in order to adapt it to the legislative changes concerning Whistleblowing ▪ Updated §1.2.2
5.0	17/03/2021	▪ Formal review following the regulatory evolution ▪ Company Organization Chart update ▪ Comprehensive review in order to adapt to legislative developments	▪ Adaptation to the provisions that came into force following the issue of law no. 3/ ▪ Update of the section dedicated to the description of the organizational structure of the Company ▪ Amendment of articles 24 and 25 of L. Decree 231/2001 ▪ Update of the list of offenses to the new criminal offenses introduced in L. Decree 231/2001 ▪ Introduction of art. 25-*quinquiesdecies* in L. Decree 231/01, entitled "Tax offenses" and other regulatory changes

Summary

1 GENERAL SECTION

1.1 Legislative Decree No 231/2001

Legislative Decree 231/01 ("*Regulations on the administrative liability of legal persons, companies and associations including those which are unincorporated...*", dated 8 June 2001) establishes the principle through which some collective bodies (hereinafter also referred to as "*Entities*") are responsible, in the manner and within the terms indicated, for crimes committed by Staff belonging to the corporate structure - crimes which are specifically indicated in the Decree itself.

From the clear viewpoint of making the Entity accountable for proper managerial organization, a valid defense factor that the legal entity can use in the circumstances where a crime has been committed through which the organization pursues an unlawful interest or benefits from an unfair advantage, arises from its ability to demonstrate that it has absolutely no involvement in the criminal facts as an institution, with the consequent attribution of liability and/or interest solely to the agent party which committed the crime.

Said non-involvement must be proven by demonstrating that the internal organization operates in a watchful manner, taking a preventive stance both in terms of forming a proper decision-making structure and in terms of supervising the lawful use of corporate financial resources.

With L. Decree 231/2001, the principle through which legal entities also answer directly for crimes committed for their benefit or to their advantage, by those working professionally for them, was thus incorporated into our legislation.

The Entity's liability for sanctions and the related overall functionality of the preventive system, designed to avoid the attribution of responsibility, are concepts related to the interpretation ability of the legal person's internal organization and the resulting proper constitution both of preventive ethical standards and of surveillance rules which are "defensive" in relation to the facts (such as in fact, those contained in the "*Organization and management models*"), which the Directors have a statutory obligation to make provision for, including in the interest of the company's assets.

The abovementioned assessment also reviews:

- internal surveillance measures over the "organization and management models" established;
- the set-up of designated bodies provided with appropriate powers;
- acknowledgement of the existence or not of specific features to evade the aforesaid measures, in relation to the facts in question, by those who have committed crimes despite the preventive measures.

The essence of the legislation in question implies that if the crime is committed by people "*belonging*", under the terms specifically established by the Decree, to the legal entity, the occurrence of the crime may also directly lead to the applicability of various consequential and severe penalties to the Company, in addition to the typical "consequences" which will affect the offender.

The primary practical effect of the decree is therefore the extension of the scope of liability for committing certain crimes.

The party which has derived a benefit – including an economic one – from an unlawful act, is validly assumed to pay for the consequential legal liabilities, which supplement and do not replace any statutory consequences, or those based on the impacts of damage to third parties.

This reflection of liability shall commence as soon as certain individuals belonging professionally to the Entity become the originators of certain specific crimes, hereinafter also called "*underlying crimes*".

Therefore, the issue has an impact upstream of a selective analysis both on the Parties which determine the liability and on the unlawful acts which lead to their occurrence.

As far as "internal" Parties are concerned, the law provides for the following:

1. individuals who hold representation functions;
2. individuals who hold administration functions;
3. individuals who hold functions relating to the management of the Entity or of its autonomous organizational unit (a secondary office, for example, but also a plant or a representative office);

4. individuals who exercise even de facto management or control of the Entity itself;
5. individuals subject to the direction or supervision of any Party mentioned in the points above (which corresponds to a significant extension of the scope in question).

The Decree lays down that the liability of the Entity is not triggered if it is legally demonstrated that the natural persons listed above have committed the crime giving rise to the derived implication of the legal person acting solely in the party's own interest or in the interests of outside parties.

There are two subjective types of Party which are relevant: senior management and subordinates.

A senior management position is essentially one which gives rise to the assumptions that we have included in points 1 to 4 above. It is in fact those Parties which, under the Decree, are addressed as a priority by the regulation on the exempting capacity of what we refer to below with a term that is already in vogue in practice, the "protective shield" (i.e. the set of measures which aims to prevent the "transmission" of liability which is at the crux of the Decree). With regard to the relationship between "senior management" Parties and the "shield", it is important to emphasize how, for the "shield" to be effective, in the case of crimes committed by these Parties, it is necessary to prove in court that, in committing the crime, they acted with malice even towards the *shield*, i.e. they have voluntarily and fraudulently failed to comply with the requirements and content of the "*Organization and management model*".

It must also be proved, in addition to what concerns the action of the "lawbreakers", that there has not been an absence of or an insufficient supervision by the appropriate "Supervisory Board" as regards the operation, the observance and the updating of the Model.

For Parties which are subject to the management of others (Employees or Collaborators who are not in senior management positions), notwithstanding the fact that they also do not transmit liability to the Entity if they act, with regard to the crime, exclusively in their own interest or in the interest of third parties, liability is attributable to the Entity only if the occurrence of the crime was made possible by a failure to comply with the managerial and supervisory obligations, something which is excluded presumptively by the adoption and effective implementation, before the crime is committed, of a model *capable of preventing crimes of the same type as the one that occurred*.

As concerns crimes from which the liability of Entities arises (hereinafter often referred to also as "*underlying crimes*"), Legislative Decree 231/2001 identifies the following standard types:

a) misappropriation of funds, fraud against the State, a Public Body or the European Union to obtain public funds, computer fraud against the State or a Public Body and fraud in public supplies
b) computer crimes and unlawful processing of data
c) organized crime crimes
d) embezzlement, extortion, inducement to give or promise undue benefit, corruption and abuse of office
e) counterfeiting in relation to currency, public credit cards, revenue stamps and instruments or identifying marks
f) crimes against industry and commerce
g) corporate crimes
h) crimes for the purposes of terrorism or of subversion of the democratic order
i) practices involving the mutilation of female genitalia
j) crimes against individuals
k) market abuse
l) involuntary manslaughter or serious/severe personal injury, committed with infringement of the rules on health and safety protection at work
m) receipt, laundering and use of money, goods or utilities sourced illegally and also self-laundering
n) crimes relating to breach of copyright
o) inducement not to make statements or to make fraudulent statements before the judicial authority
p) environmental crimes
q) employment of third-country nationals whose stay is illegal
r) fraud in sports competitions, illicit operation of betting activities or betting and gambling carried out by means of prohibited devices
s) racism and xenophobia
t) tax offenses

u) smuggling
v) *transnational crimes* (aiding and abetting, international tobacco smuggling, illegal immigration)

Finally, it should be noted that in most cases, possibly also incorporating other types of sanction, the Entity responsible for the occurrence of a particular crime may be subject to one or more of the following *prohibition sanctions*:

a) prohibition to trade;
b) suspension or withdrawal of authorizations, licenses or concessions functional to committing the crime;
c) prohibition from entering into contracts with the public administration, except for obtaining the benefits of a public service;
d) exclusion from benefits, financing, subsidies or contributions and possible withdrawal of those already granted;
e) prohibition from advertising goods or services.

If the Entity or one of its operating units is permanently used for the *unique* or *predominant* purpose of allowing or facilitating the occurrence of crimes for which its liability is presumed, the permanent ban on exercising its business activity is always imposed.

Lastly, pursuant to Art. 23, of L. Decree 231/01 "*1. Anybody who, when carrying out the activity of the entity to which a sanction or a precautionary prohibitory measure has been applied, transgresses the obligations or prohibitions related to such sanctions or measures, is punished with imprisonment from six months to three years. 2. In the case referred to in point 1, the entity for whose interest or advantage the offense was carried out is liable to a monetary sanction of between two-hundred and six-hundred quotas and the confiscation of the profit in accordance with article 19. 3. If the entity has made a significant profit from the offense referred to in point 1, prohibitory measures are applied, including others than those previously imposed.*".

1.2 The Company Engineering. D.HUB

Engineering.MO S.p.A. was born from Engineering's acquisition of the company T-Systems Italia S.p.A., previously wholly owned by T-Systems International GmbH.

In September 2016, Engineering.MO acquired the business branch of Engineering Ingegneria Informatica S.p.A. dedicated to the management of the Data Center structure, of the IT infrastructures and of the operational activities.
On July 26, 2017, the Extraordinary Shareholders' Meeting approves the change of the company name which becomes Engineering. D.HUB S.p.A.

1.2.1 *Governance System*

Engineering. D.HUB S.p.A. (or "*the Company*" or "*the Firm*") has adopted the traditional *governance* system, which provides for the following management and control bodies:

- *Board of Directors*
- Board of Statutory Auditors.

1.2.2 *Organizational structure*

The organizational structure of Engineering is broken down into business areas according to a model based on a General Department, within which each operational office is called to operate in one or more market segments, by making use of appropriate levels of management autonomy.

The *General Department* is made up of several subordinate technical organizations (Production Departments) and is flanked by several Commercial General Departments (Commercial Departments), all hierarchically subordinate to the General Director.

Within the technical organization, inside the individual production units, responsibility for individual orders is entrusted to the *Project Heads/Service Managers*. The following General Departments operate within Engineering:

- *General Department for Finance* (banking and insurance market)
- General Department for Public Administration and Health (hereinafter also "General Department for P.A. and Health": Central government and local authorities, Public companies and Community institutions, Hospitals and healthcare authorities, University polyclinics)
- General Department for Energy & Utilities and TELCO (utilities market: electricity, gas, environmental hygiene, provision of solutions and services for leading international telecommunications carriers)
- General Department for Industry and Services (metallurgical, chemical, pharmaceutical and automotive industries, consumer products, transportation, services, etc.)

This introduction was necessary in order to frame the recent organizational evolution of Engineering.MO which, after the transfer of the Managed Operation business unit of Engineering and the new name as Engineering D.HUB (hereinafter also E.D.HUB), became the Group Engineering company that offers technological and infrastructural services to all market sectors, with a wide spectrum of solutions, flexibility in its operating model and expertise on individual customer scenarios and processes gained in over 20 years of experience in the field of Managed Operations.

Engineering D.HUB's offer focuses on the management of technological infrastructures and Cloud Services and makes use of an integrated network of Data Centers located throughout the country in Aosta (Pont-Saint-Martin), Milan, Turin and Vicenza in order to meet the highest safety standards.

The Organization is oriented towards the constant evolution of the technological solutions offered to the Engineering Customer base.

Engineering D.HUB's organization chart is structured under the guidance of a CEO as follows:

- *Business Budget&Control: Organization aimed* at supporting the economic governance of the organization and at defining and implementing transversal processes within the organization in harmony with what is defined by the Engineering group
- *Transformation, Techology Partenrship & Alliance*
- *Information Security Manager*
- *Technology Office*

And a Delivery organization which is divided into 5 Departments:

- *Solutions, Portfolio & Business Development:* Organization responsible for the design and development of the company's offer portfolio. The solution of new opportunities and major contract renewals falls under its responsibility.
- *Sales Specialists:* Organization responsible for the commercial management of the E.DHUB offer portfolio. It operates both independently and in cooperation with the commercial functions of the Group for the various markets, in order to extend the business.
- *Clients & Project Management:* Organization aimed at managing existing contracts. Responsible for the P&L of the assigned customer portfolio as well as for the development of new opportunities for managed Customers.
- *Cloud & Technology Services:* Delivery organization responsible for the provision of traditional Cloud and Data Center services, on-site or on-center management system services and innovative services, as well as for the evolution of customer infrastructure configurations.
- *Business & User Services*: Delivery organization responsible for providing services related to end users, such as Service Desk, Fleet Management and Digital workplace, as well as Robotic Process Automation projects.

In addition to the organizational structure described above, the following centralized Departments operate at Group level:

- *General Department for Administration, Finance and Control*
- *General Department for Human Resources & Organization*
- *General Department for Technical Research and Innovation*
- *Marketing Department*
- *Corporate Social Responsibility Department*
- *Corporate Security Department*
- *Processes and Internal Audit Department*
- *"ENRICO DELLA VALLE" IT & Management School.*

And finally the Functions of:

- *Data Protection Officer*
- *Compliance for the prevention of corruption*

and the *Protection and Prevention Service*

Further summary information in relation to some of the abovementioned Departments is provided below.

General Department for Financial Administration and Control is divided into the following Organizational Units (hereinafter also "*OU*"):

- Administrative Department
  - Administrative Services Center
  - Parent Company Financial Statements Department
  - D. Hub and other Italian Subsidiaries Financial Statements Services
  - Foreign subsidiary Financial Statements Department
  - Italian subsidiary Financial Statements Department
  - Tax Services Department
  - Financial services
- Legal and Corporate Affairs Department
  - Tenders Office
  - Contract management
- Consolidated Financial Statements, Planning and Management Reporting Department
- Purchasing and General Affairs Department
- IT Consultancy Purchasing Department
- Area Controller
- Debt Collection Department
- M&A Department
- Personnel Administration Department

- The General Department for *Human Resources & Organization* is structured in the following OUs:

- Industrial Relations and Organization Department
- Human Resources Management Department Northern Area
- Human Resources Management Department Central-Southern Area
- Compensation & Benefits, International Mobility Department
- Talent Development Area
- Personal Data Protection Service
- Business Data Management and Analysis
- Internal Information Systems Department
- Health, Safety and Environment Service

The General Department for Technical Innovation and Research, in addition to undertaking innovative, high-profile design activities, also manages research projects financed partly or wholly by the European Union or by other Public Bodies.

The General Department is divided into the following Departments:

- Research and Development Department
- Excellence Center Department (Exc)
- ESL Excellence Centre Department
- *ESL*[1]Projects and Consulting Department
- *ESL* AM, International Projects and cc Host Department
- ESL Methodologies, Processes and Services Department
- Data Analytics Exc Department
- PMO/PM Exc Department
- Engineering Interactive
- Architecture and Intelligent Systems Department
- ECM Competence center Department

And in staff

- Technical Offer Engineering Department
- Technology Partnership & Alliance Manager

The *Internal Auditing Service* operates under the Processes and Internal Audit Department. Its main task is to implement a check on whether the protocols laid down by this *Model* are being respected by the various OUs of the Parent Company and by the various Subsidiary Companies, in order to underpin:

- the reliability and integrity of the financial and operational accounting information
- the effectiveness and efficiency of operations
- the safeguarding of assets

[1] ESL: *Engineering Software Laboratories*

- compliance with laws, regulations and contracts.

Internal Auditing is also required to report the main results and criticalities which arise both to the Company's Senior Management and, on request, to its control and supervision bodies: *Board of Statutory Auditors and Supervisory Board* (pursuant to L. Decree 231/01; see below "*Supervisory Board*").

The Processes and Internal Audit *Department* is also responsible for:

- managing and maintaining certifications acquired by the company:
  - ✓ UNI EN ISO 9001:2015 – Quality System
  - ✓ ISO-IEC 20000–1:2011 – ICT services management
  - ✓ ISO-IEC 27001: 2013 - Information Security Management Systems with extension to the guidelines:

    ISO27017 Guidelines for information security controls in Cloud

    ISO27018 Guidelines for protecting PII in Cloud ISO27035 Guidelines for Information security incident management
  - ✓ ISO22301 - Business Continuity Management Systems

  including therefore the management of periodic internal audits within the Company's various OUs;
- maintenance of reference corporate procedures and documents within the context of certified systems.

The General Department for Human Resources & Organization is instead responsible for managing and maintaining the certification of the Environmental Management System (ISO 14001) and the Occupational Health and Safety Management Systems (ISO45001)

1.2.3 ***Company Profile***

Engineering is one of the main players in the field of digital transformation of public and private companies and organizations, with an innovative offer for the main market segments. The Group (which also includes Engineering D.HUB) with its subsidiaries is committed to pushing the envelope for the application of emerging technologies. It works in the area of system implementation and integration and on redefining processes in order to promote innovation for the benefit of businesses and Public Administrations. With around 12,000 professionals in 65 locations spread across Italy, Belgium, Germany, Norway, Republic of Serbia, Spain, Sweden, Switzerland, Argentina, Brazil and the USA, Engineering manages projects in over 20 countries, supporting clients in the business areas where digitalization is having the biggest impact.

Its products and services cover all strategic sectors, including Digital Finance, Smart Government & E-Health, Augmented Cities, Digital Industry, Smart Energy & Utilities, Digital Media & Communication.

The group aims to help change the way in which the world lives and works, by combining technological infrastructures organized in a single hybrid multicloud, the capability to interpret new business models and specialist expertise in all next-generation technologies: Artificial Intelligence, Advanced Data Analytics, Cyber Security, Robotics, Digital Twin, IoT, Blockchain.

The Parent Company *Engineering - Ingegneria Informatica SpA*, founded in 1980, was listed on TechSTAR, the stock market segment dedicated to shares with high capital and financial requirements, until July 2016, when the PTB procedure was completed with the consequent delisting of the Company's shares.

For an updated and more detailed description of Engineering Group, please see the "*Group Profile*" which can be found on the Group's website (**www.eng.it**), in the section: *who-we-are/engineering-group/*.

The Company Engineering D.HUB S.p.A. has never been subjected to proceedings pursuant to L. Decree 231/01.

1.3 Code of Ethics for Engineering Group

The *Engineering Group Code of Ethics*, starting from the heritage of values shared by all the Group's Companies, establishes the rules of conduct which all those who, whether directly or indirectly, temporarily or permanently, establish collaborative relationships in any capacity or who operate in the interests of the Group, must apply when carrying out their business and in managing corporate activities.

The *Engineering Group Code of Ethics* must therefore be considered binding for Directors, Managers and all Employees, members of the control bodies (*Board of Statutory Auditors*), members of the Supervisory Board, temporary or permanent external Employees, Partners, Suppliers and Clients.

The *Engineering Group Code of Ethics* is an integral and substantial part of this *Organization and Management Model*. Therefore breaches of its provisions represent violations of the *Model*, with all the consequences arising therefrom in relation to the applicability of disciplinary sanctions.

1.4 The Company's organization and management model pursuant to Legislative Decree 231/01

A system of preventive controls considered appropriate for ensuring that the risks of the crimes envisaged by Decree 231/01 occurring should be reduced to an "acceptable *level*", is defined as a system which, if circumvented, leads to *fraudulent behavior* on the part of whoever carries out the unlawful act.

The abovementioned system is divided into specific sector-based protocols (*procedures*) consisting of a set of preventive and subsequent controls, which are an integral part of the *Organization and management model* and an indispensable tool intended to guide the activities of "sensitive" Parties.

It is believed that the *Organization and management model* implemented possesses the connotations of an effective system of preventive control, characterized by the existence of the following features, which include fundamental *principles of control*:

- an organizational system that is sufficiently formalized with specific reference to the allocation of functions, responsibilities and hierarchical reporting lines;
- the separation, independence and integration between corporate functions: the various stages within a single process (execution, operative control, accounting, supervision, authorization, etc.) may not be managed autonomously by a sole person;
- powers of authorization and signature which are formalized and consistent with the functions and responsibilities held by Parties working in senior management roles
- manual and computerized control points;
- the verifiability, traceability and appropriateness of each corporate process, in particular of the most significant transactions and operations
- the verifiability, traceability of the control activities: *operative* (foreseen in the context of the process) or *supervisory* (first and second level, where foreseen)
- the continuous disclosure to the Supervisory Board of information concerning at-risk operations and the timely provision of information to said Board in relation to anomalies or violations of the organizational model
- monitoring by the Supervisory Board concerning the implementation of the organizational Model.

1.4.1 Corporate documents included within the Model

The following corporate documents must be considered an integral and substantial part of this *Organization and management model*, including in relation to the consequences concerning applying disciplinary measures to any possible infringement of the provisions contained therein:

- *Code of Ethics for Engineering Group* (which has already been referred to)
- the *Safety of Workers Management System Manual*
- the Corporate Procedures, Protocols, Regulations and Guidelines referenced by the abovementioned documents and those duly invoked by this *Model*

are all available on the corporate intranet (if not for public access on the Group's website **www.eng.it** in the "*Investor Relations*" - "*Corporate Governance*" section).

1.4.2 Methodology for definition and revision of the Model

A summary description of the operational phases undertaken for defining the initial establishment of the *Organization and management model* is provided below, with a reference also to the subsequent revision phases. We focus in particular on the description of the steps followed for drawing up the second section of this *Model*, the *Special Section*, which describes each underlying crime, placing it within the Corporate context, and provides references to the standards, protocols and controls put in place to defend against the risk of a crime occurring.

1.4.2.1 Analysis of the underlying crime and identification of the possible methods for committing a crime

Legislative Decree 231/2001 regulates the liability of an *Entity* (legal entities, companies and associations including unincorporated ones) in relation to administrative crimes dependent on the occurrence of specific crimes. The "*underlying crimes*" listed in the Decree, since its adoption, are varied and were subsequently added to several times, with the addition by the Legislator of new and more advanced cases.

In the approach followed for defining the *Organization and management model*, the first objective set was to identify the actual risk of a crime to which the Company was exposed being committed.

This primarily required a careful *technical-legal* analysis of the crimes referred to by the Decree. This process was in fact evaluated as an essential prerequisite for the specific identification of risks that are actually detectable in the Company, with this being our prime objective, as mentioned above.

The subsequent step to the concrete identification of the criminal behavior referred to by the Decree is to recognize - in some cases even putting some "imagination" to work in doing so - the possible methods and circumstances by which one or more Individuals, operating within the Company's organization, could engage in *this* criminal behavior.

Following the outcome of the risk analysis, it was considered advisable not to include in the Model the Special Sections related to the hypotheses of underlying crime which are not realistically achievable within the corporate context (such as the case of "mutilation practices of female genital organs" laid down in Article 583-bis of the Criminal C. referred to in Article 25-quater 1 of the Decree).

1.4.2.2 Identification of the processes, the Parties and the sensitive OUs

Based on the identification (sometimes even *theoretical*) of the methods through which a specific underlying crime could be committed, the outcome of the previous phase, the next stage is the recognition, basically in a concurrent manner, of the following:

- corporate processes and sub-processes in which criminal behavior could most easily be achieved;
- the Parties and/or OUs that are most "sensitive" or exposed to the risk of committing the crime.

This phase is essentially aimed at *mapping* the risks on the one hand and the processes and sensitive OUs on the other. It has proved to be very effective also insofar as it has provided elements which complement and enhance the previous phase. Indeed, a more detailed analysis of the processes carried out within individual corporate functions has often led to highlighting a new way in which a crime could occur, which was previously not recognized; and starting from this, new processes and new sensitive OUs *which* previously escaped the analysis, were identified.

The cyclical interaction between these two initial phases has thus allowed achieving a sufficiently accurate mapping, which would have been difficult to achieve ([2]) had such phases been executed just once in sequence.

1.4.2.3 Assessment of the level of defense against at-risk processes

Once a sufficiently complete view of the following has been attained:

- the actual risks (of underlying crimes) which the Company may be exposed to occurring,
- the processes, the Parties and the OUs that are *sensitive* to such risks.

we finally analyzed what level of "risk protection" was offered by the existing corporate standards and by currently in-place *procedures*. (hereinafter with the term "*procedures*" we will refer both to the documents which govern specific corporate processes and, synthetically, to the entirety of the protocols described and provided for within these documents).

It must be said that given the nature of the crimes referred to in the Decree, for many of them it was shown to be entirely appropriate to refer primarily to the *principles*, *standards of behavior* and *values* expressed in the *Code of Ethics for Engineering Group*; while for some underlying crimes, the "shield" was by itself sufficient to avert the occurrence of a particularly reprehensible crime, characterized by a high negative social value.

In most cases, possibly to integrate that point in the Code of Ethics, for each process which revealed itself sensitive to a specific risk of a crime, a review of the existing business processes was carried out, in order to verify *whether* and *to what extent* they offered adequate *protection* in terms of the prescribed rules and checks, both *preventive* and where applicable, *subsequent* to implementing a particular business process or one of its phases.

In cases where such protection was absent (or was deemed insufficient), new versions of the procedures concerned have also been updated and issued, in order to make them suitable for providing protection against the specific risk.

In some cases where, despite insufficient protection, it was not deemed appropriate to make provision, for example, for issuing a specific procedure, the rules and controls needed to protect against the risk of a particular crime occurring have been directly included, *with equal prescriptive efficacy*, within the *Special Section* of this *Organization and management model*.

At the end of the review of the corporate processes and with reference to a specific crime, it has emerged that the protocols and effective controls (including *indirect ones*) against the risk of a crime occurring are often very numerous and described in detail. To make the *Model* easier to read, we chose to group controls and protocols, detailed in this manner, into standard groups by similarity of context and purpose, summarizing each group in a *summary description* of standards, protocols and controls (see below), a description identified in the *Model* by the code "*Prot. Id.*".

The detailed content of a particular protocol (set out in the *Model*) - and of its controls - is always available:

- by accessing reference corporate documents, duly indicated;
- by consulting a voluminous document (for internal use) which shows, for each "*Prot. Id.*" quoted in the *Model*, the protocols and detailed controls required within the Company.

With reference to this second point, it should be noted that the abovementioned document, for internal use:

- is kept constantly updated;
- contains detailed controls which are taken into consideration by Internal Auditing when conducting its institutional activities, by checking their effective implementation, including for the benefit of the Supervisory Board.

([2])… even by exploiting, as occurred, the possession of a thorough knowledge of the corporate organization by those who carried out this analysis. This is due to the multiplicity of functions and processes found in a company as large as Engineering. D.HUB.

In conclusion, within the *Special Section* of the *Model*, the following items have therefore been listed for each underlying crime:

- a *summary description of the crime* and, where necessary, several examples of the same
- the *corporate context*: sensitive OUs/processes and possible methods of committing the crimes
- the *description of the prescribed corporate behavior,* the standards and protocols
- a *summary description of the controls applied*
- *the references to corporate documents* containing the standards and protocols.

1.4.2.4 Revision of the Model

This *Organization and Management Model* is subject to regular checks, especially from the perspective of effectiveness in relation to the objectives for which it has been prepared and in order to guarantee an effective implementation of the provisions of the *Model*. During these verification activities, the main role is played by the *Supervisory Board* (described in detail below), which may use, in this regard, the information contribution provided to it by the Processes and Internal Audit *Department*.

Events that may lead to the revision of the *Model* are as follows:

- the occurrence of significant violations of the provisions of the *Model* (or the procedures it refers to), such as to highlight, even indirectly, a vulnerability to the risk of a specific crime being committed;
- changes in the organization of the Company or in corporate processes, where the one and/or the others may require an update of the "mapping" of the three entities – the risk of crime – the sensitive Parties or OUs – the sensitive processes/sub- processes – and, therefore, a review of the standards, protocols and controls to provide for protection against risk;
- changes or additions to Legislative Decree 231/01 implemented by the Legislature, with the introduction of new underlying crimes (not previously included) or with modifications concerning crimes already provided for by the Decree.

In all cases, regardless of the motivation that triggered the process of revision of the Model, the three operational phases that led to the first draft of the Model, as previously described, are replicated.

Each revision of the *Model* shall obviously be followed by the phases of approval and publication discussed below.

Please note that *simply* changing one or more of the documents referred to in the *Model* (referenced in the Special Section of this document) does not constitute a "*revision of the Model*". Those who, when applying the provisions of this Model, are required to refer to the documents referred to herein, must access the latest version of these on the company's intranet.

1.4.3 Approval and publication of the Model

For the purposes of its enactment, this *Organization and management model* is subject to approval by the Company's Board of Directors ("*BoD*").

In the event of a revision of the *Model*, where the changes are not aspects that are considered to be particularly urgent, such approval shall occur at the time of the first functional *Board of Directors* meeting. Otherwise the Chief Executive, possibly at the request of the *Supervisory Board* or of the Processes and Internal Audit *Department* Head, convenes an early dedicated *Board of Directors* meeting for approving the new version of the Model.

Once approved, the *Organization and management Model* is published on the company intranet.

The enactment of a new version of the *Model* is always accompanied by a contextual internal information release, sent via e-mail and addressed to all Employees, which signals the availability of the new version on the company's intranet and provides a summary of the reasons behind the update.

1.4.4 Recipients and scope of the Model

The Decree stipulates that the Entity is considered liable in the event of crimes committed in its interest or to its advantage by the following Parties:

- Individuals who perform representation or administration functions;
- Individuals who perform management functions for the Entity or for one of its autonomous Organizational Units (for example, a secondary office);
- Individuals who exercise management or control over the Company, even on a de facto basis;
- Individuals subjected to the direction or supervision of any Party mentioned in the points above.

In addition to these Recipients, which are predominantly but not *necessarily* Employees of the Company, all nevertheless operating within the framework of activities performed by the corporate organization, all those who have established relationships with Engineering D.HUB (whether governed or not by a contractual relationship) such as Clients, Partners and Suppliers, shall be required to comply with the rules and principles referenced by this *Model* .

It is stressed in particular that the principles, standards and protocols referenced by this *Model* should also be observed within the context of activities carried out in countries outside Italy, in the name of or on behalf of *Engineering D.HUB S.p.A.*

1.5 The Supervisory Board

1.5.1 Assumptions behind its creation

L. Decree 231/2001 sets out that the adoption of an organization and management model be accompanied by the identification and creation of a special *Supervisory Board* (hereinafter also *"SB"*).

More specifically, such a body is governed by Article 6 of the decree in question, pursuant to which the Entity is not liable for crimes that may be committed even or only in the interest of or to the benefit of the Entity itself, where the latter can prove, among other things, (a) that a sound organization model was previously adopted; (b) that "*the task of supervising the operation and the observance of the models and of their update was entrusted to an organization within the Entity equipped with autonomous powers of initiative and control*".

In substance, based on Article 6, the so-called "*protective shield*", which should shelter the Entity from the consequences arising out of a crime carried out by a Party holding a *senior* management position (as defined by the Decree), is created both by a sound organization and management model and by the establishment of an appropriate *Supervisory Board*.

On the other hand, as far as crimes committed by so-called *Non-managerial* Parties (as defined by Article 5, paragraph 1, letter b of Legislative Decree 231/01), it must be reported that the identification or establishment of such a regulatory body is not required with equal clarity. In reality, however, it must be noted that Article 7 of said Decree, which specifically regulates crimes committed by non-managerial Parties, sets out that the model, in order to be in a position to properly protect the Entity, should be effectively implemented, then indicating that the effective implementation of the model requires, among other things, "*a regular check and the possible amendment of the same when significant violations of provisions are discovered or when changes in the organization or the activity occur*". It is clear therefore that this periodic checking will be conducted by a suitable Supervisory Board.

1.5.2 Requirements of the Supervisory Board and of individual members, grounds for ineligibility and forfeiture

The requirements which must characterize a Supervisory Board, based on the interpretation of Art. 6 of L. Decree 231/01, are described below:

a) **Autonomy and independence**: the Board must be autonomous and independent from the Entity's governing bodies, in order that it may fully carry out its role. This autonomy and independence not only require the absence of any form of hierarchical subordination, but also the fact that operational and decision-making powers are not granted. In fact, the presence of such powers in relation to the board might, in some cases, prejudice and compromise the abovementioned autonomy and independence requirements, causing an unacceptable overlap between the controller Party and the controlled one.

b) **Internal character of the Body**: as is clear from Art. 6 of L. Decree 231/01, the supervision functions placed under the remit of the Board cannot be fully allocated externally, not even through *outsourcing* dynamics. This does not however mean, as clarified below, that it cannot make use of external consultants, whose presence ensures that there is autonomy and independence from Senior Management.

c) **Professionalism**: the Board must be equipped with adequate powers and skills which are appropriate in ensuring that there is effective performance of the supervisory tasks envisaged by Decree 231/01. In the event of a control body which is formal in nature, this entails the selection of members with the knowledge and professionalism required to perform the functions, including knowledge of the Entity's internal structure, competencies in company, organizational and purely legal or criminal matters. Still in relation to a control body which is formal in nature, this necessary professionalism can also be achieved through recourse to one or more external consultants.

d) **Continuity of action**: the constant surveillance and control activity required by L. Decree 231/01 dictates that the body in question be able to ensure a sufficient degree of continuity in the action it takes. This therefore means that such a body is called on to be continuously in operation, and, where necessary, constantly present within the company.

Parties in possession of the professional qualifications required for carrying out the functions and/or who have completed specific experience in the company context shall be eligible for membership of the Supervisory Board. In particular, the skills required relate to legal, economic, financial, corporate and organizational matters.

Members of the Board may hold functions or offices within the company, provided that these do not lead to their holding individual operational managerial powers that are incompatible with exercising the functions of the Board.

The following constitute grounds for ineligibility as members of the Supervisory Board:

- the conviction, even at first instance, or the determination of the penalty requested pursuant to Articles 444 et seq. of the Code of Criminal Procedure for one of the crimes envisaged by Legislative Decree 231/2001;
- the conviction, even at first instance, involving the banning, even temporary, from public office, or the temporary banning, from executive office, of legal persons and companies;
- the conviction, even at first instance, or the determination of the penalty requested pursuant to Articles 444 et seq. of the Code of Criminal Procedure for crimes against the public administration, financial crime, or for crimes that may in any case affect the Party's moral and professional reliability;
- the legal condition of being banned, incapacitated or bankrupt;
- the exercise or potential exercise of an activity competing with or conflicting with the interests of the activity carried out by the Company.

The members of the Supervisory Board must declare under their own responsibility that they are not in any of the situations constituting ineligibility or in any other situation of conflict of interest with regard to the functions/tasks of the Supervisory Board, pledging, should one of these situations occur (and without prejudice to the absolute and irrevocable obligation to abstain under such circumstances), to notify the Board of Directors immediately in order to allow their replacement in the role.

The following constitute grounds for forfeiture of members of the Supervisory Board:

- the conviction at second instance or the determination of the penalty requested under Articles 444 et seq. of the Code of Criminal Procedure for one of the crimes envisaged by L. Decree 231/2001;
- the conviction at second instance to a sentence involving the banning, even temporary, from public office, or the temporary banning, from executive office, of legal persons and companies;
- the conviction at second instance or the determination of the penalty requested under Articles 444 et seq. of the Code of Criminal Procedure for crimes against the public administration, financial crime, or for crimes that in any case may affect the Party's moral and professional reliability;
- the legal condition of being banned, incapacitated or bankrupt;
- the exercise or potential exercise of an activity competing with or conflicting with the interests of the activity carried out by the Company;
- the non-disclosure of a situation of incompatibility or of conflict of interest with respect to the functions/tasks of the Supervisory Board or the violation in such circumstances of the obligation to abstain.

1.5.3 Term of office and termination

At the time of the appointment of the Members of the Supervisory Board, the Board of Engineering D.HUB established that they should remain in office until their revocation, approved by the Board itself.

The termination of the term of office of members of the Supervisory Board is determined - aside from revocation – by waiver, expiry, permanent impediment and, as concerns internal Company members appointed as a result of the corporate function they hold, through no longer holding that function.

Any waiver by members of the Supervisory Board may be exercised at any time and must be communicated to the Board of Directors in writing, together with a statement accounting for its reasons. The waiver takes immediate effect if a majority of the members of the Board remains in Office, or otherwise, from the moment that the majority of the Board is reconstituted, following acceptance of the new members.

Revocation of the mandate to one or more members of the Supervisory Board can be decided by the Board of Directors, having heard the non-binding opinion of the *Board of Statutory Auditors*, for just cause.

Just cause for revocation is defined as follows:

- a serious failure to fulfil their duties/functions, as defined in the Model;
- the Company's conviction, pursuant to the Decree, including by a measure that has not yet become final, justified on the basis of the "absence of or insufficient supervision" by the Board;
- the occurrence of one of the grounds for revocation;
- the breach of the prohibition of communication and dissemination of information.

In the event of termination of a member of the Supervisory Board for whatever reason, the Board of Directors shall proceed, without delay, to replace the member by special resolution. In that case, the replacement member stays in office until the expiry of the term of the other members of the Supervisory Board.

In the event of the termination of the Chairperson's term of office, his/her functions are taken over by the eldest member until the acceptance of the new Chairperson.

The Supervisory Board and each of its members, as well as those individuals which the Supervisory Board shall make use of to perform its functions (whether these Parties are internal or external to the Company), shall not suffer retaliatory consequences of any sort as a result of the work performed.

1.5.4 Convocation, voting and deliberations

Meetings of the Supervisory Board shall be convened by the Chairperson or at the joint request of the other members, and shall be valid with the presence of the majority of its members.

The deliberations of the Board shall be taken by an absolute majority and accounted for, expressly indicating any minority position.

Each member of the Board is obliged to give notice to the other members of any conflict of interest with an activity of the Board, whether directly or on behalf of third parties, in particular specifying its nature, terms, origin and extent and in any case refraining from participating in the deliberations concerning the activity in question. In the event that a member should have been delegated an activity, said individual must refrain from fulfilling it and refer the matter to the full Board.

1.5.5 Information retention and prohibition from communication

A paper and/or electronic copy of all material related to the activity carried out is kept by the Technical Secretary of the Board for a minimum period of ten years.

To this end, the Company equips the Board with structures suitable for filing the material indicated above.

Access to the archive by third Parties must be authorized in advance by the Board and take place in accordance with the rules which it has laid down.

On appointment of the data controller, in respect of the management of the e-mail box and of the paper and electronic archives, the members of the Board take on the title of personal data processing managers pursuant to European Regulation no 2016/679 and adopt all appropriate precautions to preserve said data, ensuring that there is a regular backup of data on a quarterly basis.

Members of the Supervisory Board, Members of corporate structures and any Consultants employed, shall not disclose or disseminate news, information, data, deeds and documents acquired whilst pursuing their activities, without prejudice to the disclosure obligations provided by the *Model* and by the provisions in force.

1.5.6 Regulations of the Supervisory Board and reports for Senior Management

The Supervisory Board approves its own regulations which govern how it operates.

The Supervisory Board reports the results of its activity in a half-yearly written report sent to the Chief Executive Officer. The Supervisory Board also sends an annual report to the Board of Statutory Auditors.

In order to perform specific control activities, the Supervisory Board shall have access to the *Internal Auditing* function, which prepares the annual plan of internal actions to be taken within the Company at the start of the year.

1.5.7 Functions and powers of the Supervisory Board

In accordance with the provisions of L. Decree 231/01, the Supervisory Board is entrusted with the following functions:

a) to monitor the real efficacy and effectiveness of the *Organization and management model*, in relation to the prevention of the crimes referred to by Legislative Decree 231/01;

b) to ensure that the *Organization and management model* and *Code of Ethics* are complied with;

c) to oversee the continued appropriateness of the *Organization and management model* in relation to any change in the corporate structure and/or of the regulatory framework which may have occurred and to take care of any update.

In order to ensure the effective and efficient performance of the aforesaid duties and to comply with Article 6, paragraph 1, letter b), of L. Decree 231/01, the Supervisory Board is granted the following powers:

- to issue the provisions deemed necessary for surveillance and control activities, as well as for activating the information channels referred to in the paragraphs below;
- to collect and file any information and/or news deemed useful and relevant for the purposes of the decree in question;

- to perform, including possibly by using sampling methods, every appropriate check or investigation on transactions, acts or conduct carried out within the Company;
- to make use of external consultants with a proven professional track record;
- to process the information and news collected, the items received through the information channels referred to in the paragraphs below, as well as the results of any investigations and checks carried out;
- to draw up proposals for change, update and/or implementation of the organization and management Model or Code of Ethics as may be considered appropriate;
- to accomplish whatever is considered appropriate for the dissemination of knowledge concerning the organization and management Model within the Company, as well as among external Parties (external Collaborators, Suppliers and Partners) who may come into contact with the Company;
- to notify any violation of the *Model* in writing to the Board of Directors and the *Board of Statutory Auditors*;
- to develop, in coordination with the General Department for *Human Resources & Organization*, adequate methods for personnel training as concerns the decree in question (without prejudice to the General Department for *Human Resources & Organization* having exclusive jurisdiction over the implementation of the methods developed);
- to develop, in coordination with the Business Departments and the General Department for Financial Administration and Control, the appropriate contractual clauses for a better regulation, pursuant to the decree in question, of relations with Third parties (without prejudice to the exclusive competence of the Business Departments and of the General Department for Financial Administration and Control for the concrete implementation of the contractual clauses developed);
- to freely access documentation that is useful for achieving the institutional aims of the Supervisory Board held by different company departments, the Directors and the Board of Statutory Auditors;
- to periodically receive from the Parties specified in this Model the information identified in the '*Information flows*' paragraph;
- to promote, without prejudice to the competence of senior management for imposing sanctions and the related disciplinary proceedings, the application of any disciplinary sanctions, including in the case of failure to send the requested *Information flows* to the Supervisory Board;
- to coordinate the monitoring of activities in relation to the principles established by the *Model*, including with the support of the various corporate functions, by calling specific meetings where appropriate.

In order that it may tangibly carry out its functions and effectively exercise its powers, in compliance with the prerogatives of *autonomy* and *independence* which characterize it, the Supervisory Board is assigned a *consistent* expense budget by the Board of Directors, aimed at ensuring the effective performance of its duties (e.g., specialist consulting, travel, etc.).

1.5.8 Notification requirements

The Supervisory Board is the recipient of information flows concerning the implementation of the *Organization and Management Model* and the *Code of Ethics*, according to the information channels activated pursuant to Article 6, paragraph 2, letter d), of Legislative Decree 231/01.

Employees of the Company and, in particular, "*Internal parties responsible for the supply of information flows pursuant to L. Decree 231/01*" identified within the Company (hereinafter for brevity referred to as: "*Persons in charge of the 231 information flows*") have an obligation to forward the following information to the Supervisory Board:

- measures and/or information from the Public Administration from which the performance of investigations is inferred, including in relation to persons unknown (see Article 8 of L. Decree 231/01), for one or more of the crimes referred to in that decree;
- requests for legal assistance forwarded by managers and/or employees in respect of any prosecution taking place for one or more of the crimes envisaged by Legislative Decree 231/01;
- reports drawn up by the Managers of each corporate Department, from which facts, deeds and behaviors, including omissive, may arise, potentially relevant pursuant to L. Decree 231/01;

- information concerning the establishment and completion of disciplinary proceedings, including any penalties imposed and archiving measures taken, in relation to the infringement of the *Organization and management model*.

Furthermore, in order to ensure that its duties are properly exercised, the Supervisory Board must be informed, by anyone who may become aware, of all information concerning the following:

- the implementation of the *Model* within the Company, including with reference to the application of the protocols;
- the possible existence of areas of activity fully or partly devoid of regulation;
- any weakness in the system;
- the identification of potential anomalies in the application of the *Model*;
- integration proposals and changes to operational procedures or to the *Model* itself;
- violations or suspected violations of the *Model*, the procedures referred to therein or the *Code of Ethics*;
- the Company engaging in operations of an extraordinary nature
- crimes occurring within the Company.

All communication sent to the Company's *Supervisory Board* must be in writing and may be transmitted anonymously, if appropriate, by e-mail to the 231Dhub@eng.it address, made available by the Board.

The abovementioned email inbox is accessible to members of the Supervisory Board and to the Head of *Internal Auditing* and is rendered inaccessible to Third Parties.

The Supervisory Board shall ensure that reporting Parties are protected against all forms of retaliation, discrimination and/or penalty, by guaranteeing, within the limits of the Company's legal obligations and of the protection of its rights, the anonymity of such reporting individuals and the confidentiality of what is reported.

1.5.9 Information flows towards the Supervisory Board

The Processes and Internal Audit Department, represented by the Director, or by a Party identified by the Director, notifies the Supervisory Board of checks carried out within the Company and of their outcomes in summary form.

Further, having stated that the company gives, ex officio, the role of "*Heads of information flows 231*" to General Division Managers and Central Group Managers, the *Heads of information flows 231* shall send to the Supervisory Board:

1) every four months:
   - information (of a type specifically identified) considered useful for the timely identification of *high-risk* activities (in view of L. Decree 231/01) or which is useful in documenting the correct application of the measures provided by this *Model*;
   - any other data deemed useful for the improved implementation of the *Model*;
2) two months from the end of the four-month period pursuant to the previous flow:
   - a brief update on any occurrence of relevant events and/or significant cases of non-compliance worth reporting;
3) in each case, compulsorily and immediately, data relating to:
   - the occurrence of underlying crimes and the adoption of behavior which is not in line with the rules of conduct laid down by the *Model*;
   - measures and/or information from which the performance of investigations can be deduced, including in relation to persons unknown, for the crimes referred to in the Decree which are assumed to have been committed within the Company; or the existence of criminal proceedings against the Company itself;

- requests for legal assistance forwarded by Parties against which the Judiciary is proceeding for the crimes envisaged by the Decree;
- any anomaly or inconsistency found within the scope of the activities at risk, the information relating to claimed or proven violations of the *Model* or the *Code of Ethics* and any disciplinary sanctions imposed, or archiving measures taken for those proceedings and the reasons for any decisions.

External Collaborators, Suppliers and *Partners* make any report relating to the activity carried out by the Company directly to the Supervisory Board, in the manner previously described.

The Supervisory Board:

1) guarantees the confidentiality of the identity of the reporting individual and of the individuals being reported; the reporting person is also protected against any form of retaliation, discrimination or penalization;
2) evaluates the reports received and, where necessary, performs a preliminary investigation, without being obliged to notify the decision taken to the reporting individual.

Where a violation of the *Model* is recognized, the Supervisory Board:

- instigates a disciplinary process against the Employee held liable with the appropriate Department;
- informs the Board of Directors and the Board of Statutory Auditors in the event of a breach committed by one or more members of the above-mentioned Corporate Bodies;
- calls on the competent Department to enforce the contractual termination and/or cancellation clauses in relationships with external Collaborators, Suppliers and Partners, in the case of an infringement originating with those parties.

1.5.10 Violation reports of the Model in light of the legislation on "whistleblowing"

With the approval of the draft bill no 3365-B ("*Provisions for the protection of whistleblowers who report offenses or irregularities which have come to their attention within the context of a public or private employment relationship*"), which took place on 18 October 2017, the applicability of the regulations relating to the system of protection of public employees who report offenses of which they became aware due to their employment relationship was extended to the private sector, through inclusion, in art. 6 of L. Decree 231/2001, paragraphs 2 bis, ter and quater.

Under the new legislation, the following must be reported:

(a) unlawful conduct as defined by the Decree and based on precise and consistent facts;

(b) violations of the Organization and Management Model of the entity, which the Recipients have become aware of by reason of the functions performed.

The subjects required to transmit the aforementioned reports, pursuant to art. 6, paragraph 2-bis, letter a) are:

(i) "*the persons indicated in article 5, paragraph 1, letter a)*" of the Decree, i.e. individuals who perform representative, administrative or managerial functions for the entity or for one of its financially and operationally autonomous organizational units, or individuals who exercise management or control thereof, even on a de facto basis;

(ii) "*individuals indicated in article 5, paragraph 1, letter b)*" of the Decree, i.e. subjected to the direction or supervision of any individual mentioned in letter (i) above.

The reports may relate to any corporate area relevant for the purposes of applying the Decree and the current Model and must contain:

- useful elements for reconstructing the reported fact, attaching, where possible, the relevant supporting documentation;

- information that allows, where possible, the identification of the person responsible for the reported fact;
- an indication of the circumstances of becoming aware of the reported fact.

The Decree also imposes defining one or more channels that ensure "*the confidentiality of the identity of the whistleblower when handling the reported fact" (art. 6, paragraph 2-bis, letter a), as well as " at least one alternative reporting channel suitable for ensuring, by means of computerized methods, the confidentiality of the identity of the reporting person*" (art. 6, paragraph 2-bis, letter b).

In order to implement this legislation, the Group has set up an IT application which allows its employees to provide detailed information, based on precise and concordant facts, of any illegal conduct or breaches of the Model of which they became aware by virtue of the functions performed.

The application is based on the "EQS Integrity Line" solution, and ensures that the reports are managed guaranteeing the protection of confidentiality in relation to the whistleblower' identity, in compliance with the provisions of Article 2 of Law 179/2017, in order to enable reporting any offenses of which they become aware whilst carrying out their work.

In order to ensure recipients of the new reporting system should be aware of their rights and of how the system operates, the Company has prepared the procedure "*CSW_PR_01_G_1_Procedura Gestione Segnalazioni anche anonime Whistleblowing*" made available on the corporate INTRANET, with specific communication.

It is possible to access the application in order to make a report via the Whistleblowing Reporting Portal accessible from the link: https://eng.integrityline.com/.

Alternatively, reports can be made via the e-mail address segnalazioni@eng.it

Finally, the reports can be sent by postal service, by letter delivered to the Company's headquarters, or by internal correspondence, addressed to Engineering Ingegneria Informatica S.p.A., Engineering Reporting Committee, care of the Internal Audit Department, Piazzale dell'Agricoltura, 24 - 00144 Rome; in this case, to protect the confidentiality and identity of the whistleblower, it is necessary, whenever possible, for the report to be placed in two sealed envelopes: the first one containing the identifying information of the whistleblower, and the second one containing the report itself. Both should then be placed in a third sealed envelope with the label "confidential" addressed to the Complaints Committee on the outside.

The Reporting Committee, the recipient and sole holder of the reports received, ensures the confidentiality of the information acquired and of the whistleblower's identity which is protected in every context subsequent to the report, with the exception of cases in which a criminal or civil responsibility of the reporting party may arise and of cases in which anonymity is not enforceable by law, (by way of example, criminal, tax or administrative investigations, inspections by supervisory bodies, etc.).

The Reporting Committee assesses the relevance of the reports received pursuant to Legislative Decree no 231/01, putting in place all measures deemed necessary for this purpose and, employing, where necessary, the collaboration of the competent corporate structures. Should the report prove to be founded, in whole or in part, the Reporting Committee transmits the outcome of the checks carried out to the Administrative Body or to the competent corporate structure / function, for the subsequent decisions, including in relation to any disciplinary proceedings.

The Committee keeps a paper and / or electronic copy of the reports received for a minimum period of 10 years.

The Company guarantees the protection of any reporting subject against any form of retaliation, discrimination or penalization, in accordance with the provisions of art. 6, paragraph 2-bis, letter c) of the Decree.

Therefore, the Company refrains from carrying out any "*acts of retaliation or of direct or indirect discrimination against the person making the report*" (such as, for example, dismissal, change of duties, transfers, subjecting the reporting party to organizational measures which have negative effects on his/her working conditions) "*for reasons related, directly or indirectly, to the report*".

1.5.11 Response to a crime report

Should the Supervisory Board become aware, through any information channel, of a *crime report* pursuant to L. Decree 231/01 committed within the corporate organization, the Supervisory Board activates a series of initiatives designed to detect any *weaknesses* in the *Model* that may have been exploited when committing the crime.

To this end, also making use of the support service provided by Internal Auditing, the Parties involved, in various roles, or those who have been informed of the facts that led to the crime occurring, are identified and interviewed; the phases of the relevant business processes are reconstructed; the checks prescribed by the protocols are analyzed, both those implemented (and the related evidence) and those that may possibly have been omitted.

Where, following an anonymous report, the investigation should focus on the conduct of an Employee, the latter will be informed of the matter by a person appointed by the Supervisory Board, in order to guarantee a transparent behavior by the Company and to dispel suspicions of a corporate attitude which prejudicially pins blame on the Employee.

Once a sufficiently clear picture of what happened has been obtained and the circumstances which have emerged have been evaluated, the Supervisory Board shall proceed, in each case, by taking one or more of the following initiatives:

- it shall inform the Senior Management of the occurrence, in particular the *General Department for Human Resources & Organization*, to which it will propose, if necessary, the implementation of appropriate disciplinary sanctions;
- it shall inform the other corporate control bodies, should they wish to implement autonomous initiatives;
- it shall urge the introduction into the *Model* of specific protocols (or, potentially, the modification of existing ones) in order to better ensure compliance in relation to avoiding the risk of a repetition of the occurrence;
- it shall propose specific adjustments of the training normally carried out in the Company to the *General Department for Human Resources & Organization*, adjustments focused on the risk of committing the crime in question, as well as possibly propose to that Department that they set up stricter disciplinary sanctions.

1.5.12 Appointment and composition

On 04/08/2014, the Board of Directors of Engineering D.HUB approved the appointment of the members of the *Supervisory Board* pursuant to Legislative Decree 231/01.

Each member fulfils the required conditions of autonomy, independence, integrity, professionalism and continuity of action, in addition to possessing the skills required for performing the assigned tasks.

1.6 Training and informing Personnel and external Contractors

The efficient operation of the *Organization and management model* requires that all its protocols, that is the main documents it refers to, should be subject to a wide, effective and authoritative distribution.

It is also appropriate that this communication process should be accompanied by an adequate training program aimed at staff in risk areas, in order to explain the reasoning behind the rules in terms of appropriateness, alongside the legal rationale, as well as their practical scope. This process of training and informing workers must occur by means of a system providing for adequate, clear and detailed communication which is repeated periodically.

- On the basis of the guidelines and proposals of the Supervisory Board, the General Department for *Human Resources & Organization* assesses the introduction of new and additional staff recruitment criteria that ensures that the Company will be even safer from internal crimes.
- On the basis of the guidelines and proposals of the Supervisory Board, the General Department for *Human Resources & Organization* is responsible for training personnel on the content of L. Decree 231/01, the *Organization and management model* and the Company's *Code of Ethics*.

The Supervisory Board promotes the provision of information and the training of personnel on the contents of the *Model*, in collaboration with the General Department for Financial Administration and Control, coordinating with other Company Departments from time to time involved in the application of the *Model*.

As far as staff training is concerned:

1) for newly-hired staff: a self-training document is supplied when hired concerning the content of L. Decree 231/01;

2) for all staff (whether the Parties are in *senior management positions* or not):
   - ✓ each check carried out by the Internal Auditing function at a given Organizational Unit provides for a specific training session addressed to the contact persons within the same unit, which aims to recall the importance of strict respect for the principles and rules contained in the *Code of Ethics for the Group* and in the *Organization and management model pursuant to L. Decree 231/01*, as well as to recall the types of crimes which the Organizational Unit is particularly exposed to, highlighting any new underlying crimes that may have been introduced by the legislator;
   - ✓ using a dedicated e-learning infrastructure, update courses concerning the content of the *Organization and management model pursuant to L. Decree 231/01* are periodically provided; such courses are intended mainly for Project Leaders and the Managers of Production Centers; in addition, face-to-face classroom training sessions are organized;
   - ✓ the adoption of the *Model* and of its subsequent updates is communicated to all Resources within the Company by sending an illustrative and explanatory email, following the publication of the new version on the company intranet and on the institutional website of the Group at the address **www.eng.it** in the section "***WHO WE ARE – OVERVIEW***".

The General Departments and, in particular, the General Department for Administration, Finance and Control may, on the basis of the guidelines and proposals from the Supervisory Board, introduce new and additional selection criteria for third parties entering into contracts with the Company (external Collaborators, Suppliers, Partners, etc.), in order to better safeguard the Company against the commission of offenses.

The above-mentioned General Departments, again on the basis of the guidelines and proposals received from the Supervisory Board, are responsible for informing third parties entering into contracts with the Company (external Collaborators, Suppliers, Partners, etc.) on the matter of L. Decree 231/2001 and the prevention measures adopted by the Company.

External Collaborators, Suppliers and Partners are informed, through specific contractual clauses, of their obligation to comply with the principles contained within the *Engineering Code of Ethics*, as well as of their obligation to avoid committing the crimes referred to in L. Decree 231/01, under penalty of their liability arising at a contractual level.

1.7 Disciplinary system

1.7.1 Introduction

Pursuant to art. 6, subsection 2 letter e), L. Decree 231/01, the *Organization and management model* must lay down a suitable disciplinary system which is able to punish failure to comply with said *Model*.

This is an essential factor, without which it would be difficult for the so-called "protective shield" to operate in favor of the Company in a fully-effective manner against the consequences envisaged by Legislative Decree 231/01.

Such a sanction apparatus must be effective, but at the same time fully compliant with existing labor laws in force within our legislation (in particular: Articles 2104 et seq. of the Civil Code; Article 7 of Law no 300/1970; Articles 23 et seq. of the National Collective Labor Agreement).

➢ To this end, in accordance with Article 7 of Law no 300/1970 (the so-called Workers' Statute), the General Department for *Human Resources & Organization*, in coordination with the Supervisory Board, ensures that there is full awareness of the Organization and management Model, including by its posting on the Parent

Company's website. In compliance with the aforementioned requirement contained in Law 300/70, the Company, in fact, publishes it in the Group's internet portal, **www.eng.it**, in the section: ***WHO WE ARE – OVERVIEW*** The application of disciplinary measures is independent and autonomous in respect of the outcome of any criminal proceedings.

The disciplinary system, pursuant to art. 6, paragraph 2 bis, letter d) of the Decree, also punishes the violation of the measures to safeguard those who have submitted a report according to the "Whistleblowing" system, as well as those who submit, intentionally or with gross negligence, reports that prove to be unfounded.

1.7.2 The disciplinary system for non-executive Personnel

Compliance by *Employees* with the rules of the *Code of ethics* and the *Organization and management model pursuant to L. Decree 231/01* must be regarded as an essential part of the contractual obligations they assume, pursuant to Art. 2104 of the Civil Code; therefore, any conduct in violation of the *Code of Ethics* or of the *Organization and management model 231/01* is considered a failure to comply with the primary obligations of the employment relationship and has disciplinary implications. The disciplinary process, the imposition of the sanction, the execution, dispute and appeal thereof shall be governed in accordance with the Workers' Statute and the National Collective Agreement.

In particular:

1) the employer may not take any disciplinary action against the employee without having first brought the charge and having listened to his/her defense;
2) except for the verbal reprimand, the charge shall be made in writing and disciplinary measures may not be imposed until at least 5 (five) days have elapsed, during which the employee may submit his or her justifications;
3) if the measure is not applied within 6 (six) days subsequent to those justifications, the latter shall be deemed accepted;
4) the employee may also submit his or her justifications verbally, with the possible assistance of a representative from the trade union association which he or she belongs to or authorizes;
5) the imposition of the disciplinary measure must be justified and communicated in writing;
6) without prejudice to the right to bring proceedings before a court, an employee who has been served with a disciplinary sanction may instigate, within 20 (twenty) days thereafter, even through the association which the employee is registered with or grants a mandate to, the creation, through the provincial labor office, of a conciliation and arbitration board which comprises one representative of each party and a third member chosen by mutual agreement or, failing agreement, appointed by the director of the labor office. In that case, the disciplinary sanction shall be suspended until the board has reached its judgement;
7) where the employer does not take action, within 10 (ten) days from the invitation addressed to him or her by the labor office, to appoint its representative to the board referred to in the preceding paragraph, the disciplinary measure has no effect;
8) if the worker brings the matter before the judicial authority, the disciplinary sanction shall be suspended until judgment has been reached;
9) dismissal for misconduct may be contested by the worker in accordance with the procedures laid down by Article 7 of Law 604/1966, as confirmed by Article 18 of the Workers' Statute. Dismissal for misconduct may therefore be contested before the court acting as employment tribunal, subject to revocation within 60 (sixty) days from receipt of its communication;
10) no effect of disciplinary sanctions can be taken into account once 2 (two) years have elapsed since their application.

➢ Consistently with the relevant legislative and contractual regulations, failure to observe the rules of the *Code of Ethics* and of the *Organization and management model pursuant to L. Decree 231/01* exposes Staff to disciplinary sanctions which shall be decided and implemented by the Company's *General Department for*

Human Resources & Organization, which shall evaluate its form and extent while taking the following factors into account:

- the extent to which the behavior was intentional or the degree of negligence, carelessness or inexperience highlighted;
- the Employee's overall behavior, particularly with regard to whether or not earlier disciplinary sanctions have been applied to the same person;
- the functional position and the duties of the Employee involved;
- any other circumstance connected with the violation, in particular whether it relates to crimes "*of particular significance*", which, in addition to crimes related to a failure to protect health and safety at work, also includes the following (by virtue of the types of activity carried out at the Company):
  - ✓ crimes related to relationships with the Public Administration,
  - ✓ computer crimes.

In this regard, the following may be considered guidelines which can be referred to (to be evaluated in the order in which they are shown):

- a verbal reprimand is considered applicable if the following circumstances are all true:
  - ✓ it is not obvious that the behavior was intentional or it highlights a moderate degree of negligence, carelessness or inexperience;
  - ✓ the person responsible for the conduct never previously had disciplinary measures for crimes pursuant to Legislative Decree 231/01 imposed;
  - ✓ the behavior does not relate to crimes "*of particular significance*" (as identified above);
- a penalty no milder than *dismissal with notice* is considered applicable if the following circumstances are all true:
  - ✓ it is obvious that the behavior was intentional and it highlights a high degree of negligence, carelessness or inexperience;
  - ✓ the person responsible for the conduct has already previously had disciplinary measures other than verbal reprimands for crimes pursuant to Legislative Decree 231/01 imposed;
  - ✓ the behavior relates to crimes "of particular significance"
- a penalty no milder than a written warning and/or fine and/or *suspension* is considered applicable in cases which do not fall within the abovementioned cases.

It is the responsibility of the Supervisory Board to monitor the system of penalties contained within the *Organization and management model*, as well as to develop any proposals for amendments which must be forwarded to the Board of Directors.

1.7.3 The disciplinary system for executive Personnel

If the Company's Executives are found guilty of violations of the standards and provisions contained in the *Code of Ethics* or in the *Organization and management model pursuant to L. Decree 231/01*, or where they may have violated the specific obligation of overseeing their subordinates, the most suitable measures in compliance with the criterion of proportionality referred to in Art. 2106 of the Civil Code shall be applicable against those Executives, in the manner set out by the law and by the National Collective Agreement for Industrial Executives.

1.7.4 Other protection measures

If the Directors or the Statutory Auditors of the Company are found guilty of violations of the procedures laid down by the *Organization and management model* or of adopting a behavior that is not compliant with the requirements laid down by the same *Model* or by the *Code of Ethics for the Group*, the Supervisory Board shall

inform the Board of Directors and the Board of Statutory Auditors without delay to ensure that all measures deemed appropriate and envisaged by the legislation in force are adopted.

In view of specific clauses within contracts concluded by the Company with third Parties (external Collaborators, Suppliers, Partners, etc.), any infringement by the latter of the provisions within the Company's *Organization and management model* may lead to the consequences provided for by those same clauses, including by way of example but not limited to, termination, cancellation and a claim for damages.

2 SPECIAL SECTION

2.1 Foreword

This section outlines the underlying crimes included in L. Decree 231/01 except for those which are not deemed to be feasible within the corporate context. For each type of crime:

- the reference case is described;
- a corporate contextualization is provided, where the description of the "*methods for committing"* the underlying crime arises out of the risk analysis conducted on the actual occurrence of the crime;
- the rules of conduct, protocols and detailed controls applied within the Company in order to defend against the risk of the underlying crime being referred to are briefly described, and the names of reference corporate documents are provided. Each description is identified by the code "*Prot. Id.*".

With respect to this last point, as already stated in another context, for each "*Prot. Id.*" quoted in the Model, the detailed protocols and controls required in the Company are made accessible, both by consulting the Procedures that are duly referenced and by consulting a specific document (for internal use) which lists them.

The logical sequence adopted in the paragraphs below for handling the various crimes is consistent with the sequence of Articles of L. Decree 231/01 which relate to underlying crimes.

This document will then deal with so-called "*transnational crimes*", not actually *included* in L. Decree 231/01, but introduced by Law no 146/2006 which acknowledges the *administrative liability of Entities* for the aforementioned crimes, referring to specific Articles of L. Decree 231/01.

Finally, we shall briefly focus on art 23 of the Decree entitled "*Failure to comply with prohibition measures*", which sanctions the violation of the obligations and/or prohibitions concerning sanctions or precautionary prohibition measures imposed against the entity.

2.2 General principles of behavior

- With reference to the underlying crimes considered herein, the principles, values and standards contained in the Code of Ethics for Engineering Group must be respected, in the first instance, as binding instructions, and must be considered, for all purposes, an integral part of the Organization and Management Model pursuant to L. Decree 231/01; both must be published on the company's intranet and, as concerns the Code of Ethics, also on the Group's website (www.eng.it). Their content shall be the subject of training given to Employees.
- It is absolutely forbidden in any case, for anyone acting in the name of or on behalf of the Company, to bring about, be involved in or give rise to any behavior which amounts to committing one of these crimes.
- It is essential that all activities and operations carried out on behalf of the Company should be guided by the utmost respect for the laws in force and the principles of fairness and transparency.
- Compliance with the legislation in force, as well as with the corporate procedures and protocols must be guaranteed, in relation to both the active and passive Cycles and to the management and use of resources and business assets, particularly for those which originate from outside Italy.
- A clear, transparent, diligent and cooperative demeanor must be maintained with the Public Authorities, in particular with regard to the Judicial and Investigative Authorities, through the disclosure of all the information, data and news that may be requested.

- Anyone in the Company who becomes aware of conduct by Employees/Collaborators which leads to one of the underlying crimes discussed in this document is required to notify his/her direct Manager, the Processes and Internal Audit Department and the Supervisory Board.

2.3 Misappropriation of funds, fraud against the State, a public body or the European Union or to obtain public funds, computer fraud against the State or a public body and fraud in public supplies[3] (Article 24 of L. Decree 231/01)

2.3.1 Crimes referred to by L. Decree 231/01

Article 24 of the Decree specifically refers to the following crimes.

- Embezzlement to the detriment of the State
- Unlawful receipt of funds to the detriment of the State
- Fraud against the State
- Aggravated fraud to obtain public funds
- Computer fraud against the State or other public bodies
- Fraud in public supplies
- Fraud in agriculture

The following are examples of the crime cases referred to.

- Use of contributions, subsidies or funding for purposes other than those set by the Public body which granted them
- Providing false information or omitting the information due (e.g.: at the time of the Offer/Response to a call for tenders) in order to unduly obtain contributions, financing, a reduction in contributions or similar benefits from a Public body
- Using fictitious devices or deception, inducing anyone into error in order to obtain an unfair profit, contributions, financing or similar benefits, to the detriment of the State or other Public body
- To the detriment of the State or other public bodies, gaining an unfair profit for the company or another party, by altering the operation of a computerized/electronic system or by intervening without having the right to do so, in any manner, on data, information or programs contained in a computer system or a relevant component therein.

2.3.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's exposure to risk is significant, particularly in relation to the following **sensitive Parties/OUs**:

- Gen. Dept. for PA and Healthcare
- Gen. Dept. for Technical Research and Innovation
- "ENRICO DELLA VALLE" IT & Management School.
- In fact, these OUs address market sectors which can be perfectly identified with the Parties referred to in this article of the Decree: State, Public Authorities and Community Institutions. The "ENRICO DELLA VALLE" IT & Management School and the Gen. Dept. for Technical Research and Innovation could in particular be recipients of funding, grants or subsidies supplied by Public Authorities.

[3] Indictment replaced by art. 5, paragraph 1, letter a), num. 1), of L. Decree No. 75 of July 14, 2020.

To a lesser extent, the following OUs may also be sensitive:

- Gen. Dept. for Human Resources & Organization (recruitment of staff against funding/lower contributions)
- Gen. Dept. for Administration, Finance and Control (whose offices could facilitate the completion of a crime).

The **processes/sub-processes sensitive** to risk are as follows.

- Participation in a tender: preliminary activities for formalizing the Response to the call for tender: formalizing the Response
- Subcontract management: acquisition of authorization from the Client
- Provision of supplies (e.g. training) with the use of funding or rebates from Public Bodies
- Project Management/Analysis-Revision Offer or Contract
- Project Management/Assignment of responsibility to Project Leader and training of Work Group
- Project Management/Management of relationships with Clients, Suppliers, or any Partners in a Temporary Consortium
- Project Management/Monitoring and audit, during works, of compliance with contractual requirements
- Project Management/Reporting to Funding Body of costs incurred
- Direct Recruitment and selection of Staff
- Financial incentives related to the recruitment of Staff
- Temporary Consortium Administrative Management/Management of economic relations between Partners
- Assignment and use of Proxies

The **methods for committing the crime** that can be theoretically hypothesized are as follows.

- In order to facilitate the assignment of the order, the Response to the call for tenders (or Offer) is prepared in an incomplete or not entirely truthful manner, making use of inaccuracies, omissions, falsehoods or similar devices.
- The results of the task of defining the budgeted costs and the incurred costs and of the Project Status do not stem from transparent and documentable processes.
- Performing educational programs which in terms of subject, method or teaching are not compliant with those included in the project approved by the supplying Body
- Provision of training courses to learners who do not fulfil the requirements that were indicated by the Body providing grants, subsidies or funding
- Recruitment of staff with requirements that do not comply with those which were indicated by the Body granting loans or reduced contributions
- Implementation of irregular economic payments between Partners in a Temporary Consortium
- In the context of provision to the State, to a Public or Community Body, acting illegally on information and programs relating to its Information System.
- Implementation, in bad faith, of installations or works intended for a Municipality using poor quality materials instead of those contractually provided for
- Implementation of upgrading works of the IT systems of a company which supplies public services performed with the awareness of their non-compliance with the legislation and with the content of the contract
- Delivery of a product or service other than that agreed when carrying out a supply contract with the Public Administration.

Finally, it should be noted that the Company has decided to characterize crimes committed within the context of relations (prior or subsequent to the formalization of contracts) established with a *Central* or *Local* Public Administration, or with Community Institutions, as crimes "*of particular significance*" and to penalize these with greater severity within the *disciplinary system* described in this Model.

2.3.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.3.3.1 Specific principles of behavior

- During the phase prior to the issue of a tender notice and in the tender participation phase, the staff from an Engineering Group company who are involved in any way in commercial and/or consulting activities with the Principal, must draft and update monthly reports in which they record, in summary form, all the contacts had with the Body's managers, including any informal contacts, reporting (in addition to the obvious circumstances of date, time, place and people present), the content and any results of such contacts. This evidence will be suitably filed by each report writer, to be made available on request from the Processes and Internal Audit Department or the Supervisory Board.
- In order to be fully assured that in the context of a supply to any Client, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if carried out in the Company's interest or advantage), the company Parties mandated to authorize said supply, including for aspects connected to "passive cycle" phases (such as, for example, outsourcing aimed at providing the supply), must sign a declaration which certifies: - that, on the basis of the information at their disposal and up to the date of signing the declaration in question, at no stage of the commercial negotiations or contractual formalization, have any episodes occurred which, even hypothetically, may be indirectly or directly attributed to the RELEVANT acts laid down in L. Decree 231/01; - the undertaking to immediately report to the Supervisory Board pursuant to L. Decree 231/01 any attempts, episodes or acts, even hypothetically classifiable among the crimes mentioned above, should these occur after signing said declaration, until the supply has been fully implemented.
- In the event of supplies made to the Principal by a Temporary Consortium that an Engineering Group company takes part in, it is severely forbidden to implement any tacit economic payments between the partners. Any economic payment, in whatever form, must be explicit, motivated and duly formalized.
- The formal acts of establishing a Temporary Consortium (Establishment of the Temporary Consortium, special mandate of representation, internal Agreement / Rules) may be countersigned ONLY by those holding formal power of attorney which defines, among others, any financial limits concerning the "signable" amount.
- In all cases in which the recruitment of staff determines the disbursement of public funds and/or grants, the Personnel Department is required to verify the existence of all the objective and subjective requirements necessary for the use of the funding before appointment. For each Candidate, the evaluation forms shall contain the summary of the evaluation process and must be signed by at least two Evaluators, belonging to different structures of the organization. All documentation related to the presence of the objective and subjective requirements of personnel for which the company benefits from financing facilities, must be verified by the Human Resources Department and kept by the same in special archives.
- When carrying out supply contracts concluded with the State, with a Government Authority or with a Public Utility company or one providing essential public services, the Commercial and the Technical Departments are required to perform all the necessary formalities in order to ensure that the execution of the contract complies with what has been expressly stipulated with the Client. In particular, to avoid any behavior aimed at a fraudulent action when carrying out the contract, it is mandatory that, for its entire duration, the supply should be managed according to all the control and monitoring measures that Engineering has adopted: management of contractual aspects, management of relations with parties (Customers/Suppliers/Third Parties and other Company Structures), planning the activities and

monitoring the progress, organization and execution of the supply and the management of resources must be implemented according to the provisions of the Procedure/Activity Control.

2.3.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
01 – 01	Various Managers, technicians and sales personnel, with different roles, participate in drafting the Response to a call for tenders (or Offer). Mandatory phases are planned for the formal approval of the technical content and of the expenditure and income budgets, approvals entrusted to Managers belonging to different corporate structures. The final version of the Response to the call for tenders (or Offer), including its related annexes, shall be checked, in formal and substantive terms, by the Commercial Manager involved (or, if applicable, by the Head of the Research & Development Department) before being sent to the public Body. In particular, a check is made to confirm that the Response to the tender fulfils the subjective and objective requirements requested in the tender and that it does not contain omissions, inaccuracies or untrue information.	**- PGA10 Management of Research Contributions** **- PGA03 Active Cycle Management** **- PGA04 Supply Estimate Management** **- RS03P02 Starting Closure of Activities Procedure** **- RS01P01 Contract Acquisition Management Procedure** **- PGP31 Selection for temporary work Placements**
01 – 02	The signature, by a Company Representative: - of an Offer, a *Response to a call for tender* or a Contract with a Client (active cycle), or - a Contract or an Order to a Supplier (passive cycle) results in formal documents that commit the company externally and as such, may only be carried out by those who hold a written proxy, which sets out, inter alia, any financial limits concerning the "signable" amount. Holding powers of attorney does not exempt the holder thereof from compliance with the requirements prescribed in respect of the company's internal authorization process.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management**
01 – 03	In order to minimize the risk of committing the crimes considered here, it is mandatory to fully comply with the “Management of Proxies/Powers of Attorney” procedure which lays down the rules for the assignment and use of proxies and powers of attorney used in the process of formalizing contracts. In particular, the powers of attorney may be granted by the Commercial Attorneys within the limits of their own power of attorney and under their own responsibility, solely and exclusively within the Active Cycle and in order to operate with private parties.	**- PGA14 Management of Proxies and Powers of Attorney**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
01 – 04	In the context of: → a supply for the benefit of a Public Body, or → a supply involving funding, subsidies or contributions issued by a Public Body: - the estimate of expected costs (which must be reconciled with the response to the call for tender, including as concerns the job profiles employed for the supply), - the reporting of costs incurred, - the reporting of Work Progress must derive from documented processes, during which defined and objective criteria are applied, in accordance with the requirements of the supply. The Technical Manager for the supply is required to verify and, if necessary, to have the results obtained from processes duly authorized by his/her Managers. The documentation describing the process of estimating and reporting, the details of the input information used and the results produced are filed in a place with restricted access for at least one year from the month of closure of the contract. In the context of a supply where the final beneficiary is a Public Administration or a public funding Concessionaire, the traceability of financial flows must be guaranteed, in compliance with the provisions of Law 136/10.	**- PGA10 Management of Research Contributions** **- PGA02 Passive Cycle Management** **- RS03P02 Starting Closure of Activities Procedure** **- RS03P03 Control Implementation Procedure**
01 – 05	As part of a provision that provides for the delivery of training courses with the benefit of loans, grants or contributions from a Public Body, the process of evaluation and selection of potential learners must be conducted by at least two Commissioners, based on the requirements prescribed by the Funding Body and by applying defined and objective criteria, producing proper documentation at the end of the process, which is filed in a place with restricted access for at least one year from the month of closure of the contract.	**- PGA10 Management of Research Contributions**
01 – 06	In the context of a supply which provides for loans, grants or contributions from a Public Body, all the circumstances useful for describing in detail the nature and methods of performing the activities are subject to appropriate recording. For example, in the case of providing a training course which involves funding: → name, profile/qualification, days of attendance and final evaluation of teachers; → name, profile/qualification, days of attendance and final evaluation of learners; → days/hours of lectures, subjects covered, etc. Again with reference to the case of providing a training course, the delivery to the learners of the training program in conformity with the requirements approved by the Funding Body must also be recorded. These records must be filed in a place with restricted access for at least one year from the month of closure of the contract	**- PGA10 Management of Research Contributions** **- RS02P02 Supplier Management Procedure**
01 – 07	The role of Contract Manager/Project Manager is internally assigned to a Company Employee.	**- RS03P02 Starting Closure of Activities Procedure**
01 – 08	Within the context of a supply to the State, or other Public or Community Body, the protocols provided for the underlying crimes referred to in Article 24-bis (paragraphs 1, 2 and 3) of L. Decree 231/01 (Computer crimes and unlawful processing of data) are adopted.	**- RS03P03 Control Implementation Procedure** **- PGP03 Management of Access to Business Systems** **- RGP01 Regulation for company asset utilization**

2.4 Computer crimes and unlawful processing of data (Art. 24-bis of L. Decree 231/01)

2.4.1 Crimes referred to by L. Decree 231/01

The first paragraph of Art. 24-bis of the Decree specifically refers to the following crimes.

- Unlawful access to a telematics or computer system
- Unlawful interception, impediment or interruption of computer or telematics communications
- Installation of equipment designed to intercept, impede or terminate computer or telematics communications
- Corruption of information, data and software
- Corruption of information, data and computer software used by the State or other public body or which is in any event in the public interest
- Damage to computer or telematics systems
- Damage to computer or telematics systems which are in the public interest

The second paragraph of Art. 24-bis of the Decree specifically refers to the following crimes:

- Unauthorized possession and dissemination of codes to access information or telematics systems
- Dissemination of equipment, devices or computer programs designed to damage or disrupt a telematics or computer system.

The third paragraph of Art. 24-bis of the Decree specifically refers to the following crimes.

- Falsification of a public electronic document or one which has an evidential effectiveness
- Computer fraud by the party providing electronic signature certification services.

The following are examples of the crime cases referred to:

- with reference to the cases pursuant to **the first paragraph** of Art. 24-bis of L. Decree 231/2001:
  - Entry into a computer system, internal and/or external to the Company, violating its security system or operating within it against the express or implied will of whoever has the right to exclude such person
  - Fraudulent interception, impediment or interruption of computing/telematics communications (internal or external to the Company); public dissemination by any information method, even if only partial, of the content of the communications
  - Installation, outside the cases envisaged (by laws, procedures or contracts) of equipment designed to intercept, prevent or stop computing/telematics communications (internal or external to the Company)
  - Destruction, deterioration, deletion, alteration or suppression of third-party information, data or software; or the performance of such acts on information, data or computer programs used by or belonging to the State, or otherwise in the public interest.
- With reference to the **second paragraph** of the Article in question:
  - Unauthorized retrieval, reproduction, dissemination, communication or delivery of codes, keywords or other suitable means of access to a computer or telematics system protected by security measures, whether internal or external to the Company; giving directions or instructions that are designed for that purpose, in order to gain a personal profit or to cause damage to others.
  - Retrieval, production, reproduction, import, dissemination, communication, delivery or in any case, provision, to others of equipment, devices, computer programs (including produced by others), with the aim of damaging a computer or telematics system (internal or external to the Company), or the

information, data or programs contained therein, or in order to cause the complete or partial interruption or alteration of its operation.

- With reference to the **third paragraph** of the Article in question:
  - in relation to a public or private computer document: falsification of electronic documents or, in any event, use of false electronic documents.
  - in connection with the provision of a service or the certification of an electronic signature: violation of the obligations envisaged by the law for issuing a qualified certificate, with the purpose of gaining an unfair profit for oneself or for others or of causing damage to others.

Note: an *electronic document* is defined as any electronic media that contains data or information with evidential effectiveness or programs specifically designed to process such data or information.

2.4.2 Corporate contextualization and the methods for committing the crime

Article 24-bis of L. Decree 231/01 lists, in the 3 paragraphs which it consists of, 11 distinct crimes provided for by the Criminal Code and one provided for by L. Decree no 105/2019, all relating to the IT sector.

Given the nature of its *core business*, it is obvious that the Company is particular exposed to the criminal scenario dealt with herein.

This is further reinforced by taking into account the following two sets of circumstances which are in theory able to "facilitate" the possibility that illegal acts will be carried out:

- the technical skills necessary for committing the crimes considered herein are possessed by many of the individuals who work for the Company;
- in the context of supply activities, the staff of the Company often work "inside" the IT infrastructure of their Clients, frequently having the opportunity/requirement (regulated by the contract) to access the Client's equipment and data.

The serious sanctions which the law would impose on the Company in the hypothetical case of a crime being committed would always be of two types:

- pecuniary penalties
- prohibition measures; these can range, for example, from a ban on advertising goods or services to a prohibition from entering into contracts with the Public Administration, right up to a full prohibition of activities.

Please be aware that any legal sanctions that were to be imposed on the Company would expose the company to further, highly-significant damage: *reputational damage*. Such damage would be borne by the image of Engineering Group as a whole.

It is appropriate to add that the law provides for the application, in respect of the Entity, of aggravating factors, including in terms of the sanctions, under the following two circumstances:

- if the infringement is carried out by staff acting in the role of operator/system operator
- if the information, data or information systems subject to unlawful interventions are used by the State or other public Body or in any event in the public interest.

In the light of the above considerations, the Company has decided to consider computer crimes to be "*particularly significant crimes*" and to penalize these with greater severity under the *disciplinary system* described in this Model.

It should be noted that, even if the assumption of the *interest and benefit* obtained by the Company following the occurrence of a crime (an assumption which characterizes an Entity being imputable pursuant to

Legislative Decree 231/01) should lead (implicitly) to identifying the Company's Client (in particular: its IT System, infrastructure and the information and data managed) as the injured party, as a further measure to minimize the risk of the crime occurring, this *Model*, applies the rules, protocols, and controls shown below, including with reference to its own IT System, infrastructure and the information and data managed by that System.

As a result of all the above, it follows that, as concerns the underlying crimes referred to herein, the Company's risk exposure is so pervasive that there is no particular significance in indicating specific **sensitive Parties/OUs**, without prejudice to what is specified below with reference to the types of crime referred to in the third paragraph (see below).

Similar considerations apply with regard to **sensitive processes/sub-processes**: the risk of the underlying crime considered herein being committed is pervasive and therefore cannot be associated to specific processes, again without prejudice to what is specified below with respect to the third paragraph.

The **methods for committing the crime** that can be theoretically hypothesized with reference to the cases set forth in the **first paragraph** of the Article in question.

- The IT System ("I.S.") of the Company, a Client or a Supplier, a system protected by security measures, is breached using methods and purposes which are not authorized by those who seek to protect the system.
- An unlawful intervention is made, possibly through the installation of appropriate equipment, on the flow of communication between the Company, Client or Third Party systems, which intercepts, prevents or stops that flow. The abovementioned intervention is potentially followed by the dissemination, even partial, of the content of this communication.
- Where action is taken to make third party I.S. wholly or partly unserviceable, by illegally modifying or erasing data, information or programs; or where data, information or programs are entered/sent which are:
  - ✓ present on the systems of Clients or Third Parties,
  - ✓ used by the State or other public body or in any event, in the public interest.

With reference to the cases pursuant to the **second paragraph** of the Article in question, it is appropriate to recall what was described in dealing with the crime pursuant to Article 24-bis - paragraph 1, to which we refer.

It is important to note that, with regard to carrying out authorization processes within the Company, the transfer to another person of personal access codes to the IT Information Systems (*credentials*), or the fraudulent acquisition of *credentials* of others, may constitute instrumental actions for committing other different crimes under L. Decree 231/01. Consider, for example, the authorization of an unlawful payment aimed at an attempt to corrupt.

With reference to the types of crime pursuant to the third paragraph of the Article in question, having first noted that the crime of "*Electronic fraud in the certification of electronic signatures*" does not currently appear to be even theoretically conceivable within the Company, since the type of service in question is not foreseen, in terms of the crime of "*Falsification of a public electronic document or one which has an evidential effectiveness*", the Company's risk exposure is observed especially with reference to the following **sensitive Parties/OUs**:

- Gen. Dept. for PA and Healthcare
- "ENRICO DELLA VALLE" IT & Management School.
- Gen. Dept. for Human Resources & Organization
- Gen. Dept. for Research and innovation
- Gen. Dept. for Administration, Finance and Control

The **processes/sub-processes sensitive** to risk are as follows.

- Provision of a service for the State, a Public or Community Body/Action taken on information which contributes to constituting an electronic document produced under the Client's responsibility
- Relationships with the State Administration, a Public or Community Body/Transmission of information recorded on an electronic document.

The methods for committing the crime that can be theoretically hypothesized are as follows.

- An Employee or a Consultant engaged in the provision of a service in favor of the State or a Public or Community Body, by exploiting the possession of authorizations justified by the activities envisaged by the type of service, takes action on information contained/processed by the Client's Computer System, in order to produce an electronic document whose content is entirely or partly false.
- False electronic documents are prepared in Company dealings with the Public Administration.

2.4.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.4.3.1 Specific principles of behavior

- The parties listed below are required to scrupulously comply with all rules in force, and in particular:
  - to use the allocated IT resources exclusively to carry out their activities;
  - to properly store their Company computer system access credentials, preventing third parties from obtaining these;
  - to guarantee that entry/modification operations carried out in relation to the system of authorizations/internal powers used within the Company are traceable;
  - to make use of file protection mechanisms such as periodically updated passwords, in accordance with the Company's rules of conduct;
  - to use assets protected by copyright in compliance with the rules set forth in the relative regulation;
  - to use only authorized advertising material (i.e., photographs).

- In addition to the above, Model Recipients are prohibited from:
  - using IT resources (e.g., desktop or laptop personal computers) assigned by the Company in violation of corporate rules in force;
  - making illegal downloads or sending content protected by copyright to third parties;
  - altering public or private electronic documents with evidential effectiveness;
  - accessing an IT or telematics system without authorization or remaining there against the express or tacit desire of a party entitled to exclude this action (the prohibition includes access to internal IT systems as well as access to the IT systems of public or private competitors in order to obtain information concerning commercial or industrial developments);
  - seeking out, reproducing, disseminating, communicating or disclosing to third parties: codes, keywords or other appropriate means of access to a computer or telematics system of others protected by security measures, or giving directions or instructions that are designed to allow a third party to access the IT system of others, protected by security measures;
  - unlawfully intercepting, impeding or interrupting computer or telematics communications;

- circumventing or attempting to circumvent corporate security systems (e.g.: Antiviruses, Firewalls, Proxy servers, etc.);
- leaving their Personal Computer unattended and without a *password protection;*

➢ In any context, but particularly in the context of the provision of a service to the State, or to another Public or Community Body, even where there is an opportunity to legally enter the Client's IT system ("IS") or the technological infrastructure, the applications, programs, data and information relevant to said IS, it is absolutely forbidden to intervene in any way, with the purpose of ultimately falsifying a public electronic document or one which has an evidential effectiveness. It is also prohibited to use false electronic documents.

*2.4.3.2 **Specific protocols and controls relating to corporate processes***

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
02 – 01	An IT System ("*I.S.*") is defined in terms of its technology infrastructure, its applications, its programs, its data and the information pertaining to it, regardless of whether it is the I.S. of the Company, of a Client or a Third Party. It may be *accessed* by performing *interceptions*, *queries, duplications* or *amendments* (by taking any form of action which impacts it) ***solely and exclusively*** after the required permissions have been legitimately acquired and exclusively with the use of procedures and for purposes that are consistent with the role being performed and, within the contractual context, in accordance with the contract.	**- PGT01 Privacy Management** **- MSGTD Personal Data Processing Management Manual** **- RS03P03 Control Implementation Procedure** **- RGP01 Regulation for company asset utilization** **- GT02_0 Privacy by Design by Default**
02 – 02	Anyone acting in the name of or on behalf of the Company is directly liable, in civil and criminal terms, in accordance with the regulations in force, for the use made of the corporate network, internet and email. This responsibility also extends to the violation of protected access, copyright and licenses.	**- RGP01 Regulation for company asset utilization**
02 – 03	The software application which controls the access to the Corporate Systems must be centrally managed by strictly complying with the following criteria: ==> definition of responsibility ==> separation of functions ==> restricting access to essential and strictly necessary data only, in order to ensure the safety/security of the systems, the confidentiality and integrity of data in accordance with the tasks assigned to those who have access. The application that controls access to the corporate systems must keep track of all attempts to access the system.	**- PGP03 Management of Access to Business Systems**
02 – 04	The Manager (holder of CC) of a Resource that needs to access the internal I.S. must ask, through the appropriate computer application, for the census of the new User, specifying the profile of authorizations which must be assigned to him or her. The Personnel Department must regularly notify the person responsible for managing the access system of the names of Employees/Collaborators who have stopped working in the Company, thereby asking for their user profiles to be deactivated.	**- PGP09 Human Resources Management** **- PGP03 Management of Access to Business Systems**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
02-05	The computer application which controls access to the corporate Systems must be managed centrally while respecting the stringent protection and security policies defined in the relevant Procedure. Both when operating on-site or at a Client or Supplier site, the access codes (user-ID and password) assigned to the User must be treated as *strictly personal* and must not be disclosed to anyone else. It is prohibited to take action which aims to illegally gain knowledge of personal access codes belonging to another User and/or in order to disseminate the same. If the knowledge of personal codes belonging to others should be accidentally gained, in addition to the existence of an absolute prohibition to use these, there is also an obligation to immediately inform the User who owns the codes of this fact, so that the latter can immediately change (at least) their password.	**- PGA02 Passive Cycle Management Procedure** **- PGP09 Human Resources Management** **- PGP03 Management of Access to Business Systems** **- RGP01 Regulation for company asset utilization**
02-06	Within the corporate I.S. and when using its technological infrastructure (servers, PCs, etc.) the network, the services (including e-mail) and/or the corporate applications, it is prohibited to: → acquire or disseminate any material which is illegal or contains offensive content → receive, install, disseminate or use copyrighted software (unless expressly permitted by the license terms) or software designed to circumvent or break protection systems in place against attempts to copy/duplicate such software → carry out any operation aimed at compromising the data integrity, privacy, confidentiality, security, functionality or performance of information systems (including of individual equipment), which potentially circumvents or breaks control systems → carry out any activity prohibited by the legislation in force	**- RGP01 Regulation for company asset utilization**
02-07	Network traffic should be filtered and tracked on log files, which are retained under the law to allow the Judicial Authorities to investigate possible crimes, in compliance with the legislation in force designed to protect Workers' rights. Technical personnel, who must be duly and suitably authorized by the Company, shall have access to traffic data in order to ensure the safe and optimal operation of the network and services.	**- RGP01 Regulation for company asset utilization** **- PGP30_ Procedure for Contacts with Authorities**

2.5 Serious organized crime (Art. 24-ter of L. Decree 231/01)

2.5.1 Crimes referred to by L. Decree 231/01

Article 24-ter Decree specifically refers to the following articles within the Criminal Code.

- Criminal associations
- Mafia-type associations, including foreign ones
- Political-mafia electoral exchange
- Kidnapping of individuals for the purpose of robbery or extortion
- Organizations dedicated to committing criminal acts related to the smuggling of drugs or psychotropic substances
- Crimes involving the illegal manufacture, introduction to the State, sale, transfer, detention and carrying in a public place or a place open to the public of weapons used for military purposes or war or components thereof, as well as explosives, clandestine weapons and common weapons

The following are examples of the crime cases referred to.

- Associating with the aim of committing several crimes
- Belonging to a Mafia-type organization
- Obtaining promises of votes in exchange for the payment of money
- Kidnapping an individual with a view to gaining an unjust profit for oneself or for others
- Belonging to an association which is engaged in smuggling illegal drugs or psychotropic substances

(For the last of the crimes listed above - possession/illegal trafficking of arms – please refer to the description already provided).

The organization is of a Mafia-type when those who are part of it make use of the power of intimidation by association - and of the condition of subjecting people to a code of silence which results from this – in order to commit crimes, gain management or control over economic activities, concessions, permits, contracts and public services or to make a profit or gain unfair benefits for themselves or for others, or in order to prevent or hinder the freedom to exercise voting rights or to obtain votes for themselves or for others. The provisions of this article also apply to the camorra and to other associations, whatever they are called locally, including those from countries outside Italy, which make use of intimidating force by association and pursue aims corresponding to those of mafia-type organizations.

2.5.2 Corporate contextualization and the methods for committing the crime

An analysis of the activities in whose context the listed crimes can be committed has shown that the criminal cases at arts. 416, paragraph 6, 416-ter, 630 Criminal Code, 74 Presidential Decree no 309/1990, 407 paragraph 2 letter a) no 5 of the code of criminal procedure are not applicable to the Company. These are in fact criminal cases which should be considered entirely extraneous to the business activities undertaken by the Company, and also absolutely contrary to the values and principles which have always dictated its actions, and it is not, therefore, necessary to draw up any preventive measure or to recall specific general principles of behavior in their respect.

A partly separate case should occur for matters concerning criminal association as per art. 416 Criminal Code, whose typical building blocks are based on the stability of the association, this may be inferred from the association's level of organization and from the pursuit of an associative aim consisting in carrying out a general criminal program, that is of committing an unspecified number of crimes.

The Supreme Court intervened on the specific point by defining the operation of art. 24-ter, denying the possibility of indirectly recovering the target crimes; by thinking otherwise, in fact, "*the incriminating regulation referred to in article 416 of the Criminal Code would transform, in violation of the obligatory nature of the penalty system laid down by Legislative Decree 231 of 2001, into an "open" provision, with a flexible content, potentially capable of including any type of offense in the category of underlying crimes, with a danger of unjustifiably expanding the area of potential liability of the collective entity, whose governing bodies moreover, would, thus be forced to adopt the organizational and management models envisaged by the aforementioned art. 6 of the Legislative Decree on a basis of absolute uncertainty and in the total absence of objective reference criteria, de facto cancelling all effectiveness in relation to the desired prevention measures*" (Criminal Cassation, Section VI, 20 December 2013, no 3635).

Now, excluding the thought that it might be possible for the Company and, more generally, for any lawful business concern, to behave in such a way as to constitute an association to that end, it is a matter of closely examining the risk of the company's organizational structure being used by several persons in order to carry out a series of crimes in the interest or to the advantage of said Company, an eventuality which jurisprudence often relates to art. 416 Criminal Code, rather than purely to personal complicity in several crimes.

From this view point, it is obvious that the Company cannot previously identify the risk of this happening, rather it is linked to deviance resulting from the decisions of some of its members, should they decide to exploit the organization of persons and property which is typical of any business concern, for criminal purposes.

Conceivable preventive measures are linked in the first place to the most extensive possible circulation of the corporate philosophy pursued by the Company, reaffirming to anyone working within the Company that pursuing a corporate advantage, obtained by carrying out activities which are criminally prohibited, is never

allowed and that the Company will take all measures, including radical ones, considered useful to immediately guarantee a legal and transparent situation in that sector, in the event that a well-based suspicion should come to light whereby parties operating within the company should be involved in committing criminal deeds, albeit to the advantage of the Company itself.

However, purely in order to prevent even the remotest risk that, due to the deviance of individual parties operating within the company, criminal-type organizations may in some way be facilitated from the outside through the completion of contractual agreements, it has been deemed useful to recall the basic principles and the rules of free competition – which, moreover, have always dictated the Company's business philosophy – in order to demand that these be respected.

Since organized crime offenses can also be intended to commit crimes which have already been analyzed in the individual Special Parts, it is considered advisable to specify that the areas at risk mentioned hereunder should be understood as being part of the other areas specifically identified in respect of each case dealt with in the other Special Parts of this Model.

This clarification is considered necessary for reasons strictly linked to developing a more effective Model, in line with legislation as provided by L. Decree 231/01.

That said, as concerns the underlying crimes referred to herein, the Company's risk exposure is significant, particularly in relation to the following **sensitive Parties/OUs**:

- Senior Management
- Gen. Dept. for Administration, Finance and Control
- Commercial Divisions/Departments
- Technical production departments

The **processes/sub-processes sensitive** to risk are as follows.

- Passive Cycle (purchases and supplies)
- Active Cycle (sales)

In particular, as concerns the Active Cycle:

- Participation in a tender: preliminary activities for formalizing the Response to the call for tender: formalizing the Response
- Temporary Consortium Administrative Management/Management of economic relations between partners

The **methods for committing the crime** that can be theoretically hypothesized are as follows.

- In general terms: establishing and maintaining business, economic or commercial relationships of a criminal nature with the organization of a Client, Supplier or Partner.
- Implementing irregular economic payments between partners in a Temporary Consortium, aimed at committing the offenses considered herein.
- Producing and/or selling weapon systems (or parts of weapon systems; for example: software systems used in missile launchers), where the relationship with the specific Client or the transfer/sale procedures undertaken are prohibited by laws, conventions or applicable decisions in force.

2.5.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.5.3.1 Specific principles of behavior

- During the phase prior to the issue of a tender notice and in the tender participation phase, the staff from an Engineering Group company who are involved in any way in commercial and/or consulting activities with the Principal, must draft and update monthly reports in which they record, in summary form, all the contacts had with the Body's managers, including any informal contacts, reporting (in addition to the obvious circumstances of date, time, place and people present), the content and any results of such contacts. This evidence will be suitably filed by each report writer, to be made available on request from the Processes and Internal Audit Department or by the Supervisory Board;
- In order to be fully assured that in the context of a supply to any Client, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if carried out in the Company's interest or advantage), the company Parties mandated to authorize said supply, including for aspects connected to "passive cycle" phases (such as, for example, outsourcing aimed at providing the supply), must sign a declaration which certifies:
  - that, on the basis of the information at their disposal and up to the date of signing the declaration in question, at no stage of the commercial negotiations or contractual formalization, have any episodes occurred which, even hypothetically, may be indirectly or directly attributed to the RELEVANT acts laid down in L. Decree 231/01;
  - the undertaking to immediately report to the Supervisory Board pursuant to L. Decree 231/01 any attempts, episodes or acts, even hypothetically classifiable among the crimes mentioned above, should these occur after signing said declaration, until the supply has been fully implemented.
- In the event of supplies made to the Principal by a Temporary Consortium that an Engineering Group company takes part in, it is severely forbidden to implement any tacit economic payments between the partners. Any economic payment, in whatever form, must be explicit, motivated and duly formalized.

2.5.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
03 – 01	In order to minimize the risk of committing the crimes considered herein, it is mandatory to fully comply with all corporate rules applicable to the sensitive processes which are included in the procedures listed below: → Supplier Data Management: qualification and census for new Suppliers/amendment of personal and bank details → Qualified Supplier Register Management: selection of Suppliers from the Register, evaluation of qualified Suppliers and update of the Register → Passive Cycle Management: expense authorization, drafting, contract analysis and signature, management of invoices payable and payment mandates → Active Cycle Management: verification and authorization of cost-revenue budgets, contract analysis and signature, management of invoices receivable → Client Data Management: census of new Clients/editing of personal data. In the context of a supply whose final beneficiary is a Public Administration or a Concessionaire of public funding, the traceability of financial flows, in accordance with the provisions of Law 136/10, must be guaranteed. In general, the rule which prohibits a sole person from enabling, managing, authorizing and closing a sensitive process must be respected. In particular, the authorization processes – both for purchase and sales contracts - must as a necessity formally involve at least two different Managers. The table containing the names of Managers holding power for authorizing purchase requests, a table which is used by the electronic procedure that manages the authorization cycle, must also be subject to central management control. A similar central management control must be adopted for the table containing the names of Managers who may authorize the issue of an Offer/Contract of sale. Finally, there must always be transparency and an adequate standard of documentation when performing the above-mentioned processes.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- RS01P01 Contract Acquisition Management Procedure** **- RS02P01 Management of First Supplier Qualification Procedure** **- RS02P02 Supplier Management Procedure**
03 – 02	The signature, by a Company Representative: - of an Offer, a *Response to a call for tender* or a Contract with a Client (active cycle), or - a Contract or an Order to a Supplier (passive cycle) results in formal documents that commit the company externally and as such, may only be carried out by those who hold a written proxy, which sets out, inter alia, any financial limits concerning the "signable" amount. Holding powers of attorney does not exempt the holder thereof from compliance with the requirements prescribed in respect of the company's internal authorization process.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
03 – 03	In order to minimize the risk of committing the crimes considered here, it is mandatory to fully comply with the "Management of Proxies/Powers of Attorney" procedure which lays down the rules for the assignment and use of proxies and powers of attorney used in the process of formalizing contracts. In particular, the powers of attorney may be granted by the Commercial Attorneys within the limits of their own power of attorney and under their own responsibility, solely and exclusively within the context of the Active Cycle and in order to operate with private parties. At the time of assigning a proxy, the value limits – dependent on the corporate role of the delegated person – as defined in the relevant table published on the company intranet, must in any case be respected. The model that must be used for formalizing a power of attorney can be found on the same intranet.	**- PGA14 Management of Proxies and Powers of Attorney**

2.6 Embezzlement, extortion, inducement to give or promise undue benefit, corruption and abuse of office" (Article 25 of L. Decree 231/01)

Before we deal with the details of this special section, it is considered appropriate to acknowledge an in-depth study recently carried out by the Parent Company.

In consideration of the fact that Engineering Group also includes companies with registered offices abroad and which operate outside the national territory, and in light of the new corporate structure subject to US jurisdiction, the Parent company has considered it advisable to verify the adopted Model's compliance with the anti-bribery legislation in force in the United States of America (so-called "*Foreign Corrupt Practices Act*" or "F.C.P.A.") and in the United Kingdom (so-called "*Bribery Act*").

Starting from the analysis of L. Decree 231/01, with particular reference to the cases of public and private bribery, examining the key points of the anti-bribery legislation laid down in the "F.C.P.A.", with specific reference to the so-called "*Hallmarks of effective Compliance Programs*", as well as the procedures and rules of conduct provided for by the "*Bribery Act",* the Model adopted by the Company in the part of interest (crimes against the public administration and corporate crimes), together with the system of safeguards and controls in place, totally *comply* both with national legislation and with the FCPA and the Bribery Act.

Since these are the same company procedures, this Risk Assessment can be extended, in terms of further supervision, also to Engineering D.HUB.

Through the management system for the prevention of corruption, outlined in compliance with the provisions of ISO 37001: 2016[4], as well as through the Policy for the prevention of corruption (SGPCR01), adopted by the Parent Company and by the companies of the Group, the Company undertakes to prohibit corruption in all its forms, promoting and implementing an internal regulatory system aimed at spreading the culture of legality. In 2020, the Policy defined by the Parent Company was also extended to E.D.HUB and published on the corporate website (**www.eng.it**) in the section ***WHO WE ARE – OVERVIEW.***

[4] The ISO 37001:2016 standard, "Anti Bribery Management System", was officially approved on 15 October 2016 and constitutes the *best practice* which can be used by organizations in the fight against corruption. It aims to define internationally recognized and certifiable standards with the aim of helping organizations and companies to prevent possible corruption phenomena which might emerge during business activities, developing and consolidating at the same time a culture of transparency and integrity.

2.6.1 Crimes referred to by L. Decree 231/01

Article 25 of the Decree specifically refers to the following articles of the Criminal Code.

- Bribery (art. 317)
- Corruption through performance of duty (art. 318)
- Corruption though an act contrary to official duties (art. 319)
- Corruption though an aggravated act contrary to official duties pursuant to art. 319-bis
- Judicial corruption (art. 319-ter)
- Inducement to give or promise undue benefit (art. 319-quater)
- Bribery of a person responsible for a public service (art. 320)
- Sentences for the corruptor (Art. 321)
- Incitement to bribery (art. 322)
- Embezzlement, extortion, undue inducement to give or promise benefits, corruption and incitement to bribe members of International Courts or of bodies of the European Communities or of International Parliamentary Assemblies or International organizations and officials of the European Communities and foreign states (art. 322-bis)
- Trafficking of illicit influences (influence peddling) (346-bis)
- Embezzlement (when the fact damages the financial interests of the European Union)
- Embezzlement by benefiting from the error of others (when the fact damages the financial interests of the European Union)
- Abuse of office (when the fact damages the financial interests of the European Union)

The following are examples of the crime cases referred to.

A) Omitting or delaying official acts, or implementing an official act which goes against official duties, in order to receive money or other benefits or accepting the promise thereof, for oneself or for a third party

B) For the purposes mentioned, requesting a promise or money or other benefits

C) The crime referred to in point (A) above is committed with the aim of favoring or damaging a party in a civil, criminal or administrative case.

D) By misusing the quality or powers of a public official or of a public service appointee, inducing someone to unduly give or promise (to themselves or to a third party) money or other benefits. On the same occasion, solicited by a public official or a public service appointee, money or other benefits are unduly given or promised.

E) In relation to the crimes mentioned so far:

- money or other benefits are given or promised to a public official or to a public service appointee

or

- a public official or a public service appointee is induced into committing one of the crimes mentioned above.

F) The crime cases considered herein are committed by any individual, or against any individual who, in the context of other foreign States (European Community or other), performs functions or activities corresponding to those of a public officer or of a public service appointee.

General Note. Although some of the underlying crimes referred to herein are *crimes specific* to public entities, it must not be overlooked that the same offenses could also be committed by Employees of the Company in concert with the qualified party or by those who simply carry out *public service tasks*, a role which could theoretically be held by the Employees who supply particular services for a Client of the Public Administration.

2.6.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's exposure to risk is significant, particularly in relation to the following **sensitive Parties/OUs**:

- Gen. Dept. for PA and Healthcare
- Gen. Dept. for Technical Research and Innovation

In fact, these OUs address market sectors which can be perfectly identified with the Parties referred to in this article of the Decree: State, Public Authorities and Community Institutions.

The following OUs may also be sensitive:

- "ENRICO DELLA VALLE" IT & Management School.
- Gen. Dept. for Human Resources & Organization
- Gen. Dept. for Administration, Finance and Control.

The **processes/sub-processes sensitive** to risk are as follows.

- Passive Cycle (purchases and supplies) / Drafting, authorization, and signing of contracts, Management of invoices
- Management of Acquisition of Computer Consulting
- Active Cycle/Participation in a tender: preliminary activities for formalizing the Response to the call for tender; formalizing the response
- Active Cycle/ Drafting, authorization and contract signature
- Active Cycle/Billing Management
- Temporary Consortium Administrative Management/Management of economic relations between Partners
- Cash Management/Authorization for withdrawals and inflows, Reporting
- Management of Financial Services and Treasury/Management of bank current accounts
- Management of Resources/Selection and Recruitment of Personnel
- Assignment and use of Proxies-Powers of Attorney with external value

The **methods for committing the crime** that can be theoretically hypothesized are as follows.

- With reference to the context in which a group Company comes into contact with an Official/Representative of the State administration or of a Public or Community Body or of individuals linked to these, the following activities could theoretically constitute a corrupt behavior, i.e. be aimed at gaining an undue advantage or at providing a reward for its achievement (such as for example, being awarded a public tender contract):

  a) the purchase of supplies or professional services (e.g.: hardware equipment, consultants, trainers, etc.)

  b) recruitment of personnel by a Group Company or other complacent companies

  c) the offer or donation of goods, e.g.: valuable watches, etc.

  d) Irregular economic payments between partners in a Temporary Consortium

- Another theoretically conceivable situation is the following: an Employee of the Engineering Group engaged in the provision of a service for a Public Body, by taking advantage of the functions or powers conferred upon him or her by the Client - powers which hypothetically allow that individual to insert, edit, delete or omit data and/or information which contributes to forming deeds or documents drawn up by the Public Administration - asks for himself/herself or for third parties or induces someone to offer, to himself/herself or to a third party, money or other benefits in view of an illegal intervention on the Client's IT System.

- In a situation similar to the one mentioned above, an Employee of the Engineering Group:
  - by taking advantage of the functions or the powers conferred upon him or her by the Client, induces another person to unduly give or promise money or other benefits to him or her or to a third party, or
  - solicited by a public official or a public service appointee, unduly gives or promises money or other benefits.

Finally, it should be noted that the Company has decided to characterize crimes committed within the context of relations (prior or subsequent to the formalization of contracts) established with a *Central* or *Local* Public Administration, or with Community Institutions, as crimes "*of particular significance*" and to penalize these with greater severity within the *disciplinary system* described in this Model.

2.6.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.6.3.1 Specific principles of behavior

- Cases of behavior (A, B and C) that are prohibited below remain so, that is, "***prohibited***", even if the hypothetical behavior were to be adopted in the interest or benefit of the Company.
  - A) Anyone who introduces himself/herself in the name or on behalf of an Engineering Group Company is strictly prohibited from taking actions aimed at corrupting an Official/Representative of a State Administration or of a Public or Community Body, or a Public service appointee.
  - B) Any Party that, on behalf of an Engineering Group Company, is engaged in participating in a public tender or in providing a supply in favor of a public body, is strictly forbidden to ask for themselves or for third parties or to induce someone to offer money or other benefits to themselves or to others in exchange for committing an unlawful act.
  - C) Any Party that, on behalf of an Engineering Group Company, is engaged in providing a service for a public body, is strictly prohibited from the following:
    - ✓ by taking advantage of the functions or powers of a public official or of an *Appointee of a public service* (where granted to him/her by the Client for providing the service), inducing someone to unduly give or promise money or other benefits to himself/herself or to a third party;
    - ✓ solicited by a public official or a *public service appointee*, unduly gives or promises money or other benefits;
- During the phase prior to the issue of a tender notice and in the tender participation phase, the staff from an Engineering Group company who are involved in any way in commercial and/or consulting activities with the Principal, must draft and update monthly reports in which they record, in summary form, all the contacts had with the Body's managers, including any informal contacts, reporting (in addition to the obvious circumstances of date, time, place and people present), the content and any results of such contacts. This evidence will be suitably filed by each report writer, to be made available on request from the Processes and Internal Audit Department or the Supervisory Board.
- In order to be fully assured that in the context of a supply to any Client, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if carried out in the Company's interest or advantage), the company Parties mandated to authorize said supply, including for aspects connected to "passive cycle" phases (such as, for example, outsourcing aimed at providing the supply), must sign a declaration which certifies:
  - that, on the basis of the information at their disposal and up to the date of signing the declaration in question, at no stage of the commercial negotiations or contractual formalization, have any episodes occurred which, even hypothetically, may be indirectly or directly attributed to the RELEVANT acts laid down in L. Decree 231/01;

- the undertaking to immediately report to the Supervisory Board pursuant to L. Decree 231/01 any attempts, episodes or acts, even hypothetically classifiable among the crimes mentioned above, should these occur after signing said declaration, until the supply has been fully implemented.

- In the event of supplies made to the Principal by a Temporary Consortium that an Engineering Group company takes part in, it is severely forbidden to implement any tacit economic payments between the partners. Any economic payment, in whatever form, must be explicit, motivated and duly formalized.
- In order to be fully assured that in the context of the process of selection and recruitment of staff, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if conducted in the Company's interest or advantage), in the context of the evaluation process of the Candidate, two separate statements must be signed, one by the Candidate himself/herself, the other by the Company Manager who conducted the interview, statements in which those Parties, each based on the information at their disposal, certify that the process took place in the absence of unlawful interference by Third Parties or for illegal purposes.
- The formal acts of establishing a Temporary Consortium (Establishment of the Temporary Consortium, special mandate of representation, internal Agreement / Rules) may be countersigned ONLY by those holding formal power of attorney which defines, among others, any financial limits concerning the "signable" amount.

2.6.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	**Prescribed corporate behavior, protocols and controls applied**	**Name of corporate reference document**
04 – 01	In relationships with Clients and, more precisely, with Officials or Representatives of Public Administrations (State, Public or Community Bodies), gifts or material benefits are allowed (possibly in favor of people close to them) only if such gifts fall into normal *commercial practices*, that is, if they meet both of the following conditions: A) the gift (or benefit) is of little value; B) the gift (or benefit) is not such that it appears as: → capable of influencing the autonomy of judgment of the beneficiary i.e. → aimed at encouraging or rewarding the unlawful behavior of the beneficiary in both cases, *to the advantage of an Engineering Group company*. It is therefore forbidden for anyone introducing himself/herself in the name or on behalf of a Group company, to offer or promise to Officials or Representatives of the Public Administration (State, Public Bodies and Community Institutions) gifts (or benefits) not included in *normal business practice*. Anyone who receives, from third parties, the offer or the solicitation of a gift or benefit that does not fall within normal business practice is required to inform their direct Manager and to give formal notice to the Processes and Internal Audit Department and the Supervisory Board.	**- PGA02 Passive Cycle Management** **-PGP30 Contacts with the Authority**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
04 – 02	Given: → the potential extension of the relationships between subjects hypothetically involved in a corrupt behavior, → the multiplicity of forms with which payments can be made in exchange for requested, promised or achieved illicit advantages, in order to minimize the risk of committing the crimes considered here, it is mandatory to comply with all the company rules applicable to sensitive processes included in the following procedures: → Passive Cycle Management: purchases and supplies, in particular: traceability of financial flows (Law 136/10) in the presence of a final Client belonging to the Public Administration or a Concessionaire of public funding → Management of the Acquisition of Computer Consulting Services → Cash Management: payments and reporting → Financial Services and Treasury: management of bank current accounts → Human Resources Management: Personnel recruitment and management → Temporary Consortium Administrative Management → Supply Estimate Management → Active Cycle Management: sales management. In general, the rule which prohibits a sole person from enabling, managing, authorizing and closing a sensitive process must be respected. In particular, the authorization processes – both for purchase and sales contracts - must as a necessity formally involve at least two different Managers. The table containing the names of Managers holding power for authorizing purchase requests, a table which is used by the electronic procedure that manages the authorization cycle, must also be subject to central management control. A similar central management control must be adopted for the table containing the names of Managers who may authorize the issue of an Offer/Contract of sale. Finally, there must always be transparency and an adequate standard of documentation when performing the above-mentioned processes.	**- PGA10 Management of Research Contributions** **- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- PGA04 Supply Estimate Management** **- PGA05 Cash Management** **- RS03P02 Starting Closure of Activities Procedure** **- RS03P03 Control Implementation Procedure** **- RS02P01 Management of First Supplier Qualification Procedure** **- RS02P02 Supplier Management Procedure** **- PGP09 Human Resources Management** **- PGA06 Management of Financial Services and Treasury** **- PGA13 Temporary Consortium Administrative Management** **- PGA15 Management of Acquisition of Computer Consulting**
04 – 03	The signature, by a Company Representative: - of an Offer, a *Response to a call for tender* or a Contract with a Client (active cycle), or - a Contract or an Order to a Supplier (passive cycle) results in formal documents that commit the company externally and as such, may only be carried out by those who hold a written proxy, which sets out, inter alia, any financial limits concerning the "signable" amount. Holding powers of attorney does not exempt the holder thereof from compliance with the requirements prescribed in respect of the company's internal authorization process.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
04 – 04	In order to minimize the risk of perpetration of the crimes considered here, it is mandatory to fully comply with the "Management of Proxies/Powers of Attorney" procedure which lays down the rules for the assignment and use of proxies and powers of attorney used in the process of formalizing contracts. In particular, the powers of attorney may be granted by the Commercial Attorneys within the limits of their own power of attorney and under their own responsibility, solely and exclusively within the Active Cycle and in order to operate with private parties. At the time of assigning a proxy, the value limits – dependent on the corporate role of the delegated person – as defined in the relevant table published on the company intranet, must in any case be respected. The model that must be used for formalizing a power of attorney can be found on the same intranet.	**- PGA14 Management of Proxies and Powers of Attorney**

2.7 Counterfeiting in relation to currency, public credit cards, revenue stamps and instruments or identifying marks (Art. 25-bis of L. Decree 231/01)

2.7.1 Crimes referred to by L. Decree 231/01

Article 25-bis of the Decree specifically refers to the following crimes.

- Forgery of money, expenditure and introduction into the national domain of counterfeit and altered currency
- Spending of counterfeit money received in good faith
- Falsification of revenue stamps, introduction into the national domain, acquisition, possession or distribution of counterfeit revenue stamps, counterfeiting of watermarked paper, manufacture or possession of watermarks or equipment intended for counterfeiting currency, revenue stamps and/or watermarked paper
- Using counterfeit or altered revenue stamps
- Counterfeiting, alteration or use of trademarks or distinctive marks or patents, models and drawings
- Introduction into the national domain and trading of products with fake marks

It is hereby considered sufficient ([5]) to limit ourselves solely to illustrating the last two crimes referred to.

- Where the counterfeiting or alteration or use of trademarks or distinctive marks of Italian or foreign origin, belonging to original works or industrial products takes place, or patents, industrial designs or models, whether they are of Italian or foreign origin, are counterfeited, altered or used.
- Where there is an introduction of counterfeit or altered versions of original works or industrial products with trademarks or distinctive marks, whether they are of Italian or foreign origin, into the national domain for trade purposes, for holding or for sale or for otherwise placing into circulation.

2.7.2 Corporate contextualization and the methods for committing the crime

Sensitive Parties/OUs:

([5]) See, in fact, the statement in the following paragraph, in "*The methods for committing the crime*".

- Gen. Dept. for Administration, Finance and Control
- All OUs operating within the technical or commercial field

The **processes/sub-processes sensitive** to risk are as follows.

- Cash Management
- Active Cycle (sales)

The methods for committing the crime. The occurrence of the first four crimes specifically referred to by this Article 25-bis of Legislative Decree 231/01 would, as a condition capable of setting up a significant interest or benefit to the Company (a pre-requisite for imputing the crimes pursuant to Legislative Decree 231/01), require the widespread and consistent use, in terms of value, of tools such as those referred to by the underlying crimes. Such use is extremely limited within the company in practice, which leads to the conclusion that committing the crimes under consideration is difficult to hypothesize, even *theoretically*.

As concerns committing crimes which involve false instruments or identifying marks, this situation could occur when the Company offers goods for sale that are branded with trademarks (or logos) equal to or similar to those of another Company (other than of a Company within the Group). The reference here is to a particular type of provision relating to hardware equipment: in order to refer to this specific case study, it may be concluded that the specific turnover volume and the profit potential would be so insignificant (beyond any essential ethical evaluation) as to make the potential execution of the crime "*non-profitable*".

2.7.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.7.3.1 Specific principles of behavior

Please refer to the "*General principles of behavior"* specified in paragraph 2.2.

2.7.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
05 - 01	Particular attention must also be paid when applying the protocols and checks envisaged by the Procedures: → Cash Management → Active Cycle Management The rule which prohibits a sole person from enabling, managing, authorizing and closing a sensitive process must be respected. In particular, the authorization processes for sales contracts must as a necessity formally involve at least two different Managers.	**PGA03 Active Cycle Management - PGA05 Cash Management**

2.8 Crimes against industry and commerce (Art. 25-bis.1 of L. Decree 231/01)

2.8.1 Crimes referred to by L. Decree 231/01

Article 25-bis.1 of the Decree specifically refers to the following crimes.

A) – Disruption of the freedom of industry or trade

B) - Unlawful competition with threats or violence

C) - Fraud against national industries

D) - Fraudulent trading

E) - Sale of non-genuine foodstuffs as genuine

F) - Sale of industrial products with mendacious marks

G) - Manufacture and trade of goods carried out by usurping industrial property rights

H) - Infringement of geographical indications or of designations of origin for agri-food products

Examples of the crime cases referred to are, respectively, as follows.

A) – Performing violent acts on things or using fraudulent methods to hinder or disrupt the operation of an industry

B) – Engaging in acts of competition with the use of violence or threats when conducting business

C) - Selling or putting into circulation products with names, brands or distinctive marks that have been counterfeited or altered, causing damage to the domestic industry

D) – During the course of business, delivering a moveable item to the buyer which due to its origin, source, quality or quantity, is different to the one stated or agreed

E) - Putting non-genuine foodstuffs for sale on the market while claiming they are genuine

F) – Putting original works or industrial products for sale or bringing them into circulation with names, brands or distinctive marks that are likely to mislead the buyer about the source, origin or quality of the work or product

G) – While being aware of the existence of industrial property rights, manufacturing or working industrially with objects or other goods created by usurping an industrial property right or being in breach of one. In other words, in order to make a profit with reference to the same goods, they are introduced into the national territory or offered for sale or in any event put into circulation

H) - Counterfeiting or otherwise altering geographical indications or designations of origin on agri-food products. In other words, in order to make a profit with reference to the same products with counterfeit indications/designations, they are introduced into the national territory or offered for sale or in any case put into circulation.

2.8.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's exposure to risk is significant, particularly in relation to the following **sensitive Parties/OUs**:

- Commercial Divisions/Departments
- Technical production departments

The **processes/sub-processes sensitive** to risk are as follows.

- Active Cycle (sales)
- Passive Cycle (purchases and supplies)
- Order management/Implementation of a project (internal or external)-Provision of a service to the Client

The methods for committing the crime.

With reference to the crimes listed above, referred to in points A) and B): during the preparation/presentation phases of an Offer or a Response to a Call for Tender, a commercial manager exercises violence or threats towards a competitor (possibly a "potential" competitor).

With reference to the crimes listed above, referred to in points C), D), E) and H): these crimes are not even theoretically conceivable within the corporate entity.

For the crime referred to in point F) of the previous list: please refer to what was stated, with reference to Art. 25-bis of L. Decree 213/01, in relation to committing the crimes of "false instruments or identifying marks"

For the crime referred to in point G) of the previous list: with reference to an asset or a product over which a Third Party boasts an industrial property right, where the Company unlawfully adopts one of the following behaviors (i.e. without having previously acquired an appropriate license):

- the product/asset is instrumentally used for internal purposes not directly related to the sale of its own products;
- the asset/third-party product is instrumentally used for creating an own product intended for sale or is directly integrated within a product for sale.

2.8.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.8.3.1 Specific principles of behavior

Please refer to the "*General principles of behavior*" specified in paragraph 2.2.

2.8.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
06 - 01	With specific reference to the crime referred to in point G) of the above list and, in particular, to the hypothetical supply which incorporates a Third-Party product, the following must be duly documented and authorized: - the Purchase Request relating to the required license - the Supply estimate in which a specific cost item relating to the license appears. For both documents the authorization process must involve at least two Managers.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- PGA04 Supply Estimate Management**

2.9 Corporate crimes (Art. 25-ter of L. Decree 231/01)

2.9.1 Crimes referred to by L. Decree 231/01

Article 25-ter of the Decree specifically refers to the following crimes.

- False corporate statements (art. 2621 Civil Code)
- False corporate statements set down by art. 2621-bis Civil Code

- Obstructed control, undue return of contributions, illegal sharing of profits and reserves, unlawful transactions involving shares or quotas or those of the parent company, transactions to the detriment of creditors
- Fictitious formation of capital, unjustified distribution of company assets by liquidators

  Illegal influence on the assembly, insider trading,
- Bribery between private parties
- Incitement to bribery between private parties

The following are examples of the crime cases referred to.

- With the intention of deceiving Shareholders or the public and in order to obtain for themselves or others an unjust profit, untrue facts are reported or information on the economic, equity or financial situation is omitted in financial statements, reports or other communications, in order to mislead the recipients concerning the above information, possibly causing a financial loss to the Company, Shareholders or Creditors.
- The performance of control activities by Parties (Shareholders or other corporate Bodies) that have been legally assigned is prevented or blocked.
- Directors:
  - unlawfully return (or simulate the return) assignations to Shareholders or free them from their obligations to execute these;
  - share profits or advances on profits not actually gained or allocated legally to reserves, or share reserves which cannot legally be distributed
  - buy or subscribe to shares or quotas (or shares or quotas issued by the parent company), causing damage to the integrity of the share capital or of the legally non-distributable reserves
  - carry out reductions in share capital or mergers with other companies or spin-offs, in violation of the legal provisions, causing damage to creditors.
- Assigning Directors and Shareholders spuriously create or increase the share capital
- Liquidators share corporate assets between Shareholders before paying the company's creditors, thereby causing them damage
- A majority in the shareholders' meeting is determined in order to obtain an unfair profit for oneself or others, using simulated or fraudulent deeds
- False information is spread, simulated transactions or other strategies are deployed which aim to produce a significant change in the price of unquoted financial securities, or which are capable of significantly impacting the trust that the public has in the financial stability of banks or banking groups
- In the interest of the Company, money or other benefits are given or promised to a Party belonging to another private company, in order to perform or to omit an act in violation of the obligations inherent to his/her office or to loyalty obligations.

2.9.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the risk exposure of the company is theoretically *significant* and *extensive*, involving the following **sensitive Parties/OUs**:

- Board of Directors
- Shareholders
- Gen. Dept. for Administration, Finance and Control
- All OUs operating within the technical or commercial sector.

The **processes/sub-processes sensitive** to risk are as follows.

- General and Analytical Accounting Management
- Management of accounting closing entries
- Management of the Balance Sheet
- Management of tax obligations
- Management of Financial Services and Treasury/Management of bank transactions and financial flows
- Management of fixed assets/Management of ledger and goodwill
- Management of Passive Cycle/Commercial negotiation. Contract checking and authorization, Input into analytical accounting, Management of invoices and payment mandates
- Active Cycle Management/ Preparation of offers and commercial negotiation. Contract checking and authorization, Input into analytical accounting, Management of invoices
- Management of Order/Verification and authorization cost-benefit estimates, cost-benefit Accrual
- Management of Research Order/Reporting, Advance revenues
- Cash/Payment Management, Reporting
- Human Resources Management
- Management of Transactions with Related Parties
- Management of Buying-Selling Investments and Company Branches
- Temporary Consortium Administrative Management
- Assignment and use of Proxies-Powers of Attorney with external value

As concerns the **methods for committing the crime**, it may be observed that there are many Parties who are theoretically in a position to commit these underlying crimes, just as there are many theoretical methods for committing the crime. In this sense it is necessary to refer to the legal provision according to which committing corporate crimes leads to the company being directly liable if the criminal act – committed by Parties working in senior management roles – should provide any benefit for the Company.

It must not however be forgotten that some crimes may be committed by Parties who are not working in senior management roles, with the Entity having full liability, should the willful misconduct of Subordinates be endorsed by Parties working in senior management roles, or be made possible by their negligent control.

By way of example (any list would indeed inevitably be only partial) it is possible to theoretically hypothesize, in general terms, the following methods for committing these crimes:

- one or several Directors, departing from the spirit and content of the Code of Ethics for the Group which they approved, induce one or more individuals to work to produce financial statement data, reports or corporate communication which are untrue;
- one or several Directors, failing to provide full and transparent cooperation with the Parties that have been legally assigned control activities (Members or other Corporate Bodies), induce said Parties to partial or incorrect assessments;
- Managers responsible for administrative, technical or commercial OUs implement an inadequate level of control in the structures which report to them and fail to detect the systematic production of erroneous accounting data, with a distorting impact on specific items in the financial statements (e.g.: provisions, purchase/sales cycle data related to orders, etc.);
- for the ultimate purpose of obtaining an advantage for an Engineering Group Company, offering, promising or giving unjustified money or other benefits to a Party working in another Company (directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors and liquidators of companies or private entities), including though a third party, causing the Party to fail in his/her duties of correctness and loyalty to the Company for which he/she works;

- in the scenario outlined above, irregular economic payments are made between Partners in a Temporary Consortium;
- the Sales Manager (or a subordinate) pays or promises a sum of money or other benefits to the purchasing manager of a client company in order to favor the company's products compared with those of better quality or with a better quality/price ratio of a competitor;
- an Employee of the Engineering Group pays or promises a sum of money or other benefits to the chief executive officer or to the general manager of a competing company in order that he/she should ignore a business opportunity in relation to which the company for whom the briber works has an interest;
- the Head of the Technical Innovation and Research function pays or promises a sum of money or other benefits to the Head of the same function of a competing Company in order that he/she should disclose industrial secrets such as secret information or inventions not yet patented.

2.9.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.9.3.1 Specific principles of behavior

- It is strictly prohibited for anyone introducing themselves in the name of or on behalf of an Engineering Group Company, to offer, promise or give unjustified money or other benefits, including through a third party, to a Party operating in another Company, or private entities, causing the Party to fail in his/her duties of correctness and loyalty to the Company for which he/she works, with the ultimate aim of achieving an advantage for a Company of the Group.
- During the phase prior to the issue of a tender notice and in the tender participation phase, the staff from an Engineering Group company who are involved in any way in commercial and/or consulting activities with the Principal, must draft and update monthly reports in which they record, in summary form, all the contacts had with the Body's managers, including any informal contacts, reporting (in addition to the obvious circumstances of date, time, place and people present), the content and any results of such contacts. This evidence will be suitably filed by each report writer, to be made available on request from the Processes and Internal Audit Department or the Supervisory Board.
- In order to be fully assured that in the context of a supply to any Client, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if carried out in the Company's interest or advantage), the company Parties mandated to authorize said supply, including for aspects connected to "passive cycle" phases (such as, for example, outsourcing aimed at providing the supply), must sign a declaration which certifies:
  - that, on the basis of the information at their disposal and up to the date of signing the declaration in question, at no stage of the commercial negotiations or contractual formalization, have any episodes occurred which, even hypothetically, may be indirectly or directly attributed to the RELEVANT acts laid down in L. Decree 231/01;
  - the undertaking to immediately report to the Supervisory Board pursuant to L. Decree 231/01 any attempts, episodes or acts, even hypothetically classifiable among the crimes mentioned above, should these occur after signing said declaration, until the supply has been fully implemented.
- In the event of supplies made to the Principal by a Temporary Consortium that an Engineering Group company takes part in, it is severely forbidden to implement any tacit economic payments between the partners. Any economic payment, in whatever form, must be explicit, motivated and duly formalized.
- In order to be fully assured that in the context of the process of selection and recruitment of staff, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if conducted in the Company's interest or advantage), in the context of the evaluation process of the Candidate, two separate statements must be signed, one by the Candidate himself/herself, the other by the Company Manager who conducted the interview, statements in which those Parties, each based

on the information at their disposal, certify that the process took place in the absence of unlawful interference by Third Parties or for illegal purposes.

- Directors, Senior Company Management and, in particular, the Manager responsible for preparing corporate accounting documents, the Head of Internal Audit and all the structures which these managers are responsible for must hold a fully cooperative behavior towards Parties that have legally been assigned control activities (Shareholders or other Corporate Bodies), providing real, clear, complete and timely information.
- It is forbidden for anyone to offer money or other assets to the individual members of the Board of Statutory Auditors or to Representatives of the Statutory Auditors in order to obtain their conniving behavior;
- The General Dept. for Administration, Finance and Control must notify the Supervisory Board, with adequate grounds, of one of the following events possibly occurring outside the envisaged contractual maturities: revocation of appointment of the Auditing Firm; assignment of responsibilities to a new Auditing Firm;
- The formal acts of establishing a Temporary Consortium (Establishment of the Temporary Consortium, special mandate of representation, internal Agreement / Rules) may be countersigned ONLY by those holding formal power of attorney which defines, among others, any financial limits concerning the "signable" amount.
- Anyone who is engaged, on behalf of an Engineering Group Company, in participating in a tender or in the provision of a supply, is strictly forbidden to offer, promise or give unjustified money or other benefits, including through a third party, to a Party operating in another company, or in private entities.

2.9.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
07 - 01	Anyone belonging to Companies of the Engineering Group is prohibited from communicating or using false or incomplete information or data, or which in any case does not allow representing the real economic, net asset and financial situation of the Company, when preparing and presenting financial statements, reports, prospectuses or other corporate communications.	**- PGA08 Account Closure Management**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
07 - 02	Given: → the large number of Employees who, at various levels of responsibility, are involved in producing and communicating Financial Statement data, → the multiple business processes which generate data included in flows used as input for accounting items and, therefore, for the Financial Statements, in order to minimize the risk of committing the crimes considered here, it is mandatory to fully comply with all corporate rules applicable to *sensitive processes*, included in the procedures listed below: → General and analytical accounting management: update of the chart of accounts, direct movements → Management of Accounting Closures: analysis of deviations from the previous periods and squaring → Financial Services and Treasury Management/Management of bank transactions and financial flows → Fixed Asset Management: management of assets and goodwill → Passive Cycle Management: estimate and contract verification and authorization, accrual costs, billing management and payment mandates → Active Cycle Management: estimate and contract verification and authorization, accrued revenue, billing management → Management of Research Contributions: financial reporting and accrued revenue → Cash Management: payments, reporting → Human Resources Management → Purchase/Sale of Acquisitions and Company Branches Management → Temporary Consortium Administrative Management → Management of Proxies/Powers of Attorney. In addition to the timely implementation of the corporate power proxy system in authorization processes carried out before approval of the consolidated financial statements, it is also necessary to ensure that the information generated and communicated downstream of said processes is: → correct and complete, → supported by an adequate level of documentation, with the main entries *duly* filed. Finally, the rule which prohibits a sole person from enabling, managing, approving and closing a *sensitive process* must be respected.	**- PGA10 Management of Research Contributions** **- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- PGA04 Supply Estimate Management** **- PGA05 Cash Management** **- RS03P02 Starting Closure of Activities Procedure** **- RS03P03 Control Implementation Procedure** **- RS01P01 Contract Acquisition Management Procedure** **- RS02P02 Supplier Management Procedure** **- PGP09 Human Resources Management** **- PGP17 Personnel Administrative Management** **- PGA08 Account Closure Management** **- PGA06 Management of Financial Services and Treasury** **- PGA07 Fixed Asset Management** **- PGA11 Purchase/Sale of Acquisitions and Company Branches Management** **- PGA13 Temporary Consortium Administrative Management** **- PGA15 Management of Acquisition of Computer Consulting** **- LGA01 Guidelines for Disposal of Assets**
07 - 03	A specific procedure, approved by the Board of Directors of the Parent Company, sets specific standards to be met in the process of identification, approval and execution of *Transactions with Related Parties*, such as to ensure the procedural and substantive transparency and fairness of these transactions, whether carried out directly or through Subsidiary Companies. The Procedure also applies, where applicable, to Transactions with Related Parties which include Subsidiaries, controlled directly or indirectly by the Parent Company. The Board of Directors of the latter examines in advance such operations. To this end, the Company's subsidiaries shall promptly inform the Parent Company of Transactions with Related Parties that they intend to approve, providing the necessary information and documentation in order to implement the provisions of the above-mentioned procedure.	**- Procedure for detecting and implementing transactions with related parties**

2.10 Crimes for the purposes of terrorism or subversion of the democratic order (Art. 25-quater of L. Decree 231/01)

2.10.1 Crimes referred to by L. Decree 231/01

Article 25-quater of the Decree does not specifically refer to a series of crimes, but generically refers to "*Crimes for the purposes of terrorism or subversion of the democratic order*" laid down by the criminal code and by special laws, as well as to Article 2 of the International Convention for the suppression of the funding of terrorism created in New York on 9 December 1999.

2.10.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Gen. Dept. for Administration, Finance and Control
- Technical production departments
- Commercial Divisions/Departments.

The **processes/sub-processes sensitive** to risk are as follows.

- Supplier Data Management (qualification and census for new Suppliers/amendment of personal and bank details)
- Qualified Supplier Register Selection
- Passive Cycle Management/Assessment of Supplier Offers-Estimates, Expense authorization, Contract analysis and signature
- Management of invoices payable and payment mandates
- Assessment of qualified Suppliers and update of the Register
- Active Cycle Management/Verification and authorization of cost-revenue budgets, Contract analysis and signature
- Management of invoices receivable
- Client Data Management (census of new Clients/editing of personal data)

As regards the **methods for committing the crime** it is theoretically possible to assume an interest of or a benefit to the Company (an essential requirement for imputing a crime pursuant to Legislative Decree 231/01) in relation to relationships with Suppliers or Clients operating for the purposes of terrorism or subversion of the democratic order, where these relationships were able to reciprocally fulfil the interests of the Company and those of the organization with terrorist or subversive goals.

2.10.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.10.3.1 Specific principles of behavior

Please refer to the "General principles of behavior" specified in paragraph 2.2.

2.10.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
08 - 01	In order to minimize the risk of perpetration of the offenses considered here, it is mandatory to fully comply with all company rules applicable to *sensitive processes* included in the procedures listed below: → Supplier Data Management: qualification and census for new Suppliers/amendment of personal and bank details → Qualified Supplier Register Management: selection of Suppliers from the Register, evaluation of qualified Suppliers and update of the Register → Passive Cycle Management: assessment of Supplier Offers-Budgets, expense authorization, contract analysis and signature, management of invoices payable and payment mandates → Active Cycle Management: verification and authorization of cost-revenue budgets, contract analysis and signature, accrual of costs-revenues, management of invoices receivable → Client Data Management: census of new Clients/editing of personal data. The rule which prohibits a sole person from enabling, managing, approving and closing a sensitive process must be respected. In particular, the authorization processes – both for purchase and sales contracts - must as a necessity formally involve at least two different Managers. Both types of contract must be signed by someone assigned the appropriate power of attorney, as documented in the system of Proxies, which is managed under central control. The table containing the names of Managers holding power for authorizing purchase requests, a table which is used by the electronic procedure that manages the authorization cycle, must also be subject to central management control. A similar central management control must be adopted for the table containing the names of Managers who may authorize the issue of an Offer/Contract of sale. Finally, there must always be transparency and an adequate standard of documentation when performing the above-mentioned processes.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- PGA04 Supply Estimate Management** **- RS03P03 Control Implementation Procedure** **- RS01P01 Contract Acquisition Management Procedure** **- RS02P01 Management of First Supplier Qualification Procedure** **- RS02P02 Supplier Management Procedure**

2.11 Crimes against individuals (Art. 25-quinquies of Legislative Decree 231/01)

2.11.1 Crimes referred to by L. Decree 231/01

Article 25-d of Decree specifically refers to the following crimes.

- Reduction to or retention in slavery or servitude
- Child prostitution, child pornography, possession of child pornography
- Virtual pornography
- Tourism initiatives aimed at the exploitation of prostitution involving minors
- Trading of people, purchase and sale of slaves
- Unlawful intermediation and exploitation of labor

The following are examples of the crime cases referred to above:

this paragraph will provide the analysis and description of the crime of Unlawful intermediation and exploitation of labor as laid down in art 603-*bis* of the Criminal Code.

As regards all the other crimes referred to in art 25-*quinquies* of L. Decree 231/01, their occurrence would entail activities which are not even theoretically conceivable within the corporate context and which, in any event, would not satisfy the condition of being of interest or benefit for the Company.

The crime referred to in art. 603-*bis* of the Criminal Code, recently amended by Law no 199 dated 29 October 2016 (which came into force on 4 November 2016) punishes, unless the fact constitutes a more serious offense, "*anyone who: 1) employs workers for the purpose of setting them to work with third parties in a condition of exploitation, taking advantage of the workers' need; 2) uses, hires or employs workers, including through the intermediation activity referred to in paragraph 1), subjecting workers to exploitation conditions and taking advantage of their state of need*".
Should the facts be committed "*through violence or threat*", the punishment will be imprisonment from five to eight years and the fine from 1,000 to 2,000 euro for each worker recruited.
The fourth paragraph of the law envisages some aggravating circumstances with a special effect which result in an increase in the penalty from one third to one half: 1) should the number of recruited workers exceed three; 2) should one or more of the subjects recruited be a minor of non-working age; 3) should the fact be committed by exposing the exploited workers to situations of serious danger, taking into consideration the characteristics of the services to be performed and the working conditions.

This is a case punished by way of intent; therefore, for the purposes of the constitution of the offense, the behavior is punished only should there be awareness and the will to subject "*workers to conditions of exploitation*" taking advantage of "*their state of need*".

2.11.2 Corporate contextualization and the methods for committing the crime

As concerns the crime of "*Unlawful intermediation and exploitation of labor*", the risk exposure of Engineering concerns the following **General Departments:**

- Gen. Dept. for Human Resources & Organization
- Health, Safety and Environment Service
- General Department for Financial Administration and Control

Furthermore, the exposure to the risk of committing the crime in question, to which the Company is exposed, concerns the following **OUs:**

- Personnel Administration Department
- Human Resources Management Department Northern Area
- Human Resources Management Department Central-Southern Area
- Health, Safety and Environment Service
- Purchasing and General Affairs Department

The **processes/sub-processes sensitive** to risk are as follows:

- the management of the collaboration relationship with an employee or a self-employed worker during the establishment phase and during its execution;
- the choice and management of the relationship with suppliers, contractors, partners in relation to the application and compliance with L. Decree 81/08 on health and safety at work;
- relations with third parties that imply the use by the Entity of labor force belonging to said third parties.

As concerns the **methods for committing the crime**, the case of "***Unlawful intermediation and exploitation of labor***", merely by way of example, could take place in the hypothetical situation where the Company should recruit employees, subjecting them to exploitation conditions according to the "indices" referred to in the third paragraph of art 603-*bis* of the Criminal Code and, more precisely, according to the list contained in the norm:

- by paying the workers, in a repeated manner, salaries which clearly differ from the indications contained in the national or territorial collective agreements stipulated by the most representative national organizations and concretely applicable;

- by paying the workers, in a repeated manner, a salary that is disproportionate to the quantity and quality of the work performed;

- by violating, in a repeated manner, the regulations relating to working time, rest periods, weekly rest, mandatory leave of absence and holidays;

- by violating the rules on safety and hygiene in the workplace pursuant to L. Decree 81/08 and the provisions contained in the *Workplace Health and Safety Management System* (WHSMS -*SGSL*) adopted by the Company;

- by subjecting the worker to degrading working conditions, surveillance methods or housing.

It is necessary to clarify that should the conduct of illicit intermediation and of exploitation of labor be carried out in relation to foreign workers without a valid residence permit, the case under examination would contribute to the crime of "*Employment of citizens of third countries whose stay is irregular*" laid down in art. 25-*duodecies* of the Decree. Since these are both cases envisaged as the underlying offenses of liability pursuant to L. Decree 231/2001, their simultaneous implementation would in fact give rise to separate offenses against the Entity.

2.11.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.11.3.1 Specific principles of behavior

It is important to note how the crime of unlawful intermediation and labor exploitation, in its current formulation, punishes both the hypothesis (i) of direct recruitment of the labor force by the Company, with the aim of allocating it to work with third parties in conditions of exploitation and taking advantage of their state of need (see Article 603-*bis*, paragraph 1, no 1 of the Criminal Code), and the hypotheses (ii) of use, employment, recruitment of workers also **through intermediation activities carried out by third parties** (Article 603-*bis*, paragraph 1, no 2 of the Italian Criminal Code).

With reference to the hypotheses referred to in point (i) above, the specific behavioral principles implemented by the Company in order to prevent committing the offense are indicated below.

The competent company functions:

- when establishing the employment relationship, must guarantee workers are paid a salary in accordance with the provisions contained in the applicable national labor agreements and, in any case, proportionate to the quality and quantity of the work performed;
- must scrupulously implement the payment obligations deriving from the contracts;
- must promptly adjust the contractual provisions relating to the salary to any changes of the applicable national labor agreements;
- must adapt the scheduling of the working hours, weekly rest, mandatory leave of absence and holidays of each worker to the provisions contained in the national labor agreements which are concretely applicable; they must ensure that workers are not subjected to degrading working conditions, methods of surveillance or housing.

Given the importance, where applicable here, of the measures in the field of safety and hygiene in the workplace, in order to reduce the risks of the crime of unlawful intermediation and exploitation of labor occurring, the Recipients are required to scrupulously comply with the behavioral principles contained in the Special Section of the Model about Involuntary manslaughter and serious or severe personal injury committed by violating the rules on the protection of health and safety at work.

Please note that the violation of the rules on safety and hygiene at work is relevant for the purposes of constituting the crime referred to in art. 603-*bis* of the Criminal Code regardless of the actual occurrence of an accident and/or of the exposure of the worker to danger to personal health or safety.

With reference to the hypotheses referred to in point (ii) above, the specific behavioral principles implemented by the Company in order to prevent committing the offense are indicated below.

The competent company functions:

- must select service providers or suppliers which use labor employed through procedures that guarantee compliance with the regulations in force within the trade union context and the obligations imposed by collective bargaining agreements, as well as the rules on health and safety at work;
- must ensure that specific clauses with which the counterparty declares, under its own responsibility, to act in compliance with the regulations in force in the trade union context and, therefore, to observe, in the management of the personnel employed, the rules concerning remuneration, working hours, weekly rest, holidays, etc., as well as health and safety at work, are provided for in contracts which envisage the direct or indirect employment in any form of labor force by Engineering, supplied by these subjects;
- must ensure that specific clauses that provide for the termination of the contract in the case of breach by the contractor of the rules indicated in the previous point are included in contracts which envisage the direct and/or indirect employment in any form of labor force by Engineering supplied by these subjects.

2.11.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
09-01	In compliance with L. Decree 81/08 on the *Protection of health and safety in the workplace*, the Company supplements this Model with a regulatory system, the *Health and Safety in the Workplace Management System* ("SGSL") which provides specific legal obligations, specific protocols and procedures. The *SGSL* system is described in a *Manual* which, in addition to reporting the management rules of the System, must include, inter alia: - the mandatory nature of its observance on the part of everyone involved in the Company (Senior Management and Employees); - a commitment to fostering a culture of safety in all areas of corporate life, internal and external, including by contributing to the creation of special facilities designed to assess and, if necessary, punish conduct that violates the rules.	**- MGSL - The Safety of Workers Management System Manual** **- DC01_MSGSL01_PoliticaSicurezza 2.0**
09-02	In all cases where a contract may be involved both as a Client or with the role of Supplier, the Company must guarantee compliance with the provisions of art 26 of L. Decree 81/2008. The requirements are included in the administrative management reference procedures (ref. **PGA02_0_Gestione_Ciclo_Passivo**, **PGA03_0_Gestione_Ciclo_Attivo** and related attachments).	**- MGSL - The Safety of Workers Management System Manual** **- DC01_MSGSL01_PoliticaSicurezza 2.0**

09-03	The company establishes and maintains procedures to ensure the identification and control of potential emergencies through intervention plans that are able to: ▪ respond appropriately to emergency situations and / or potential accidents; ▪ prevent and mitigate the consequences of accidents and emergency situations. For the general characteristics of emergency management, refer to the procedure **PGS01_0_Gestione_Emergenze**. In accordance with the reference legislation, an emergency plan has been drawn up for each location (PEE ref. **SPP_*cod.Azienda*_PEE_*cod.Sede***) - disseminated to all personnel regardless of their work premises through publication on the company intranet - whose purpose is to prevent and mitigate the effects of accidental events resulting from abnormal conditions which may cause accidents, injuries or impacts on the health and safety of workers and/or of third parties in general. The emergency plan describes the organization and how to manage emergencies, including fire and first aid. The practical evacuation drill, carried out periodically as required by regulations, represents the tool through which the Company intends to ensure its preparation over time in relation to situations at risk of possible accidents. The emergency plans are subject to periodic revision during the review of the SGSL and in any case after the occurrence of emergencies or in the case of changes in the company processes which are significant for safety purposes.	**- MGSL - The Safety of Workers Management System Manual** **- DC01_MSGSL01_PoliticaSicurezza 2.0**
09-04	The 1st level monitoring has the purpose of keeping under control the preventive and protective measures prepared by the company in the field of OSH. 1st level monitoring is carried out mainly by the operator and the person in charge who, given the nature of the activities carried out in the Company, must verify: ▪ that expected behaviors are implemented (ref. **LGS01_0_Vademecum_Salute_Sicurezza,** procedures - of varying types - developed by the Company, etc.) for activities carried out at corporate premises, ▪ that the provisions provided by the host organization are complied with in the event that the activities should be carried out at third party premises. Should monitoring involve verifying specialist aspects (for example instrumental checks) it is possible to entrust this to other internal or external company resources such as MCs, SPP personnel, specialized external professionals. This type of verification includes the periodic inspections carried out by the HSO at the corporate premises, whose minutes are kept by the HSO itself.	**- MGSL - The Safety of Workers Management System Manual** **- DC01_MSGSL01_PoliticaSicurezza 2.0**

2.12 Involuntary manslaughter or serious/severe personal injury, committed by breaching the rules on health and safety protection at work (Art. 25-septies of L. Decree 231/01)

2.12.1 Crimes referred to by L. Decree 231/01

Article 25-septies Decree specifically refers to the following crimes.

- *Involuntary manslaughter* committed by breaching art. 55, paragraph 2, of L. Decree 81/08;
- *Personal Injuries* committed by breaching the laws on health and safety at work.

The following is an example of the crimes referred to.

When involuntary manslaughter is committed as a result of *wrongdoing* (negligence, carelessness or inexperience in the application of the legal rules) or an individual suffers serious or severe personal injury.

2.12.2 Corporate contextualization and the methods for committing the crime

With this type of crime, for the first time in the context of L. Decree 231/01 the liability for crimes that are "*involuntary*" (characterized by the fact that the event *was not* intended by whoever acted) is introduced. This raises a question of interpretation, noting that in this case the "*involuntary nature*" that characterizes such *involuntary* crimes (murder or serious or severe personal injury) must be reconciled with the assumption that the Company is liable, pursuant to L. Decree 231/01, i.e. with the condition that the illegal fact leads to a benefit for the Entity. This reconciliation takes place where it is noted that the failure to adopt a proper *Health and Safety at Work Management System ("*SGSL*")* could be interpreted as a "saving" for the Entity in terms of cost.

As concerns the underlying crimes referred to herein, and in consideration of the types of activity usually performed in the Company, the risk exposure for the Company is not deemed to be of extreme *statistical* significance, especially if compared with the exposure that characterizes the set of companies to which the reference standard (L. Decree 81/08 - *Consolidated Law on the protection of health and safety in the workplace*) applies.

Nevertheless, the Company has decided to consider the crimes dealt with herein as "*crimes of particular significance*" and to penalize these with greater severity within the disciplinary system described in this Model.

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Legal representative or person appointed by the Board of Directors
- Head of Gen. Dept. for Human Resources & Organization
- Head of Health, Safety and Environment Service
- Head of Organizational Unit
- Head of corporate headquarters (known as "Capo Palazzo (Office Chief)").

It is not thought possible to highlight specific **processes/sub-processes** more **sensitive** than others to the risk of the occurrence of the crimes under consideration herein.

The **methods for committing the crime** that can be hypothesized are as follows.

As a result of *negligence, carelessness* or *inexperience*, hence in the absence of the wish which would characterize malice, but the random and unintended result of pursuing a specific aim (such as for example cost containment), an accidental event occurs which leads to the death of an individual or which causes serious or severe injury.

Committing the crimes considered here could be made possible by failure to observe the *Health and Safety at Work Management System* (*SGSL*). This system, which is transposed in this model as an integral part, is specifically designed to prevent the occurrence of an accidental event such as the one just referred to. It provides for compliance with all the obligations set out in Article 30 of L. Decree 81/08, first paragraph, related to:

a) compliance with structural and technological legal standards related to equipment, facilities and workplaces;

b) risk assessment activities and preparation of measures for prevention and protection;

c) organizational activities, including emergencies, first aid, tender management, regular safety meetings and consultation with workers' representatives for safety issues;

d) health surveillance activities;

e) activities to inform and train workers;

f) monitoring activities with regard to compliance with the procedures and work instructions relating to safety which workers must follow;

g) acquisition of documentation and certificates which are required by law;

h) periodic checks on the application and effectiveness of the procedures adopted.

2.12.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

D.HUB. has adopted a specific Occupational Health and Safety Policy (DC01_MSGSL01_PoliticaSicurezza2.0) implementing an Occupational Health and Safety Management System compliant with the requirements of the ISO 45001:2018 standard in order to reiterate its own commitment and that of the entire organization to comply, in content and principles, with the laws on safety and hygiene applicable to the activities, products and services of the Company, to provide safe and healthy working conditions for the elimination of hazards, the prevention of accidents at work and the reduction of risks and to promote every initiative to prevent the occurrence of accidents which could compromise the safety of collaborators.

2.12.3.1 Specific principles of behavior

- The Internal Auditing function must carry out a 3rd level check in relation to the adoption and effective implementation of the SGSL system and of the maintenance over time of the appropriateness of the measures taken

*2.12.3.2 **Specific protocols and controls relating to corporate processes***

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
10 - 01	In compliance with L. Decree 81/08 on the *Protection of health and safety in the workplace*, the Company supplements this Model with a regulatory system, the *Health and Safety in the Workplace Management System* ("SGSL") which provides specific legal obligations, specific protocols and procedures. The *SGSL* system is described in a *Manual* which, in addition to reporting the management rules of the System, must include, inter alia: - the mandatory nature of its observance on the part of everyone involved in the Company (Senior Management and Employees); - a commitment to fostering a culture of safety in all areas of corporate life, internal and external, including by contributing to the creation of special facilities designed to assess and, if necessary, punish conduct that violates the rules.	**- MSGSL The Safety of Workers Management System Manual**
10 - 02	The *SGSL* system must provide and implement the following protocols: → compliance with the legal obligations referred to in letters (a) to (h) of Art. 30 of Legislative Decree 81/08, first paragraph, concerning: ==> a) compliance with technical and structural legal standards relating to equipment, facilities, workplaces, chemical, physical and biological agents; ==> b) the activity of risk assessment and preparation of measures for prevention and protection; ==> c) activities of an organizational nature, such as emergencies, first aid, management of contracts, periodic safety meetings, consultations with workers' representatives for safety; ==> d) the activity of health surveillance; ==> e) activities to inform and train workers; ==> f) monitoring activities with regard to compliance with the procedures and work instructions relating to safety which workers must follow; ==> g) acquisition of documentation and certificates which are required by law; ==> h) periodic checks on the application and effectiveness of the procedures adopted. → adoption of systems for recording the activities performed; → adoption of joint functions to ensure the technical skills and the powers necessary for the testing, evaluation, management and control of risk; → adoption of a system monitoring the prescribed implementation and the maintenance over time of the appropriateness of the measures taken.	**- PGA02 Passive Cycle Management**
10 - 03	Whenever, in respect of a contract for the acquisition of services, the Supplier's personnel require access to business premises or offices of our Clients (or in any case of *Third Parties*), the instructions set out in the Procedures for Passive Cycle Management and Active Cycle Management must be strictly observed, with particular reference to those that invoke obligations pursuant to L. Decree 81/2008 on the protection of health and safety in the workplace.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
10 - 04	Whenever, in respect of a supply contract, it is expected that the activities should be carried out, in whole or in part, at the Client's premises, the norms set out in the Procedures for Passive Cycle Management and Active Cycle Management must be strictly observed, with particular reference to those that invoke obligations pursuant to L. Decree 81/2008 on the protection of health and safety in the workplace.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management**

2.13 Receiving, laundering and use of illegally-sourced money, goods or utilities, as well as self-laundering (Art. 25-octies of L. Decree 231/01)

2.13.1 Crimes referred to by L. Decree 231/01

Article 25-octies of Decree specifically refers to the following crimes.

- Receiving
- Laundering
- Use of illegally-sourced money, goods or utilities
- Self-laundering (a type of offense introduced by Law no 186 dated 15 December 2014).

Some comments concerning self-laundering.

The crime of self-laundering, as laid down in art 648-ter. 1 of the Criminal Code, introduced by Law no 186/2014, punishes those who, having committed or been complicit in committing a malicious crime, use, replace or transfer into economic, financial, business or speculative activities the money, goods or other utilities resulting from the commission of said crime in such a way as to actually hinder identification of their criminal origin.

The new case of self-laundering has been included in the underlying crimes of responsibility of the Entity according to art. 25 octies of L. Decree 231/2001, with the legislator clearly intending to neutralize the economic developments of the crime carried out upstream by the guilty party, avoiding the possibility of the laundering or reuse of the unlawfully sourced proceeds being carried out by or under the cover of a legal person.

The uncertain nature of the law, together with the lack of pronouncements by jurisprudence on the matter, poses aspects which are problematic concerning the identification of the limits to which the new case applies.

The main problem hinges around the failure to identify the so-called base crimes from which the conduct typical of self-laundering can arise (art. 648 *ter*.1, in fact, generically refers to *"malicious crimes"*) and this consequently reflects on the difficulty of delineating the boundaries of the administrative responsibility of the entity.

In the aftermath of the new type of offense coming into force, there is concern as to whether the responsibility of the entity should be limited to those eventualities where the base crime of self-laundering is included in the list of presumed crimes of responsibility under L. Decree 231/2001 or whether, vice versa, it can also apply in the presence of different types of crimes, unrelated to the catalogue of crimes under L. Decree 231/2001.

We have two comments in this regard.

Firstly, the first (restrictive) interpretation would seem to be more consistent with the principle of legality and legal certainty set as the basis of the rules governing the administrative responsibility of the entity, as sanctioned by art. 2 of the Decree, whereby *"the entity cannot be held responsible for an action constituting*

a crime if its administrative responsibility in respect of that crime and the relevant sanctions are not expressly set down by a law which has come into force before the action was committed". The intent of the legislator, from the original adoption of Legislative Decree no 231/2001, was actually to establish the administrative responsibility of the entity resulting from crimes with reference to a given catalogue of criminal cases, increased in turn by subsequent legislative interventions.

Secondly, it is worth stressing that were the extensive interpretation be favored, which is intended to generate responsibility on the part of the entity for self-laundering, whatever the base crime (possibly, therefore, one not even contained in the list of presumed crimes under L. Decree 231/2001), it would be necessary to update the Organizational Model to include all malicious crimes set down by the present system, with the Model itself inevitably relapsing in terms of efficiency. In fact, the greater the number of actual crimes the Model intends to avoid, the less overall effect said Model risks having, as confirmed by memo no 19867 issued by CONFINDUSTRIA ([6]).

A similar problem has arisen in respect of cases of associative crimes (included in catalogue of crimes 231 from art. 24-*ter*), these also, due to their "open" nature, are suitable for extending the field to other criminal cases (so-called "committed crimes").

The Supreme Court of Cassation intervened by defining the effectiveness of art. 24-*ter*, denying the possibility of indirectly ascribing the liability pursuant to 231 to the target crimes; by reasoning otherwise, in fact, "*the incriminating regulation referred to in art. 416 Criminal Code would be transformed, in violation of the principle of legal certainty of the system of sanctions contemplated by Legislative Decree 231 of 2001, into an "open" provision, with a flexible content, potentially capable of including any type of offense in the category of underlying crimes, with the danger of unjustifiably expanding the area of potential liability of the collective body, whose governing bodies, moreover, would thus be forced to adopt the organizational and managerial models envisaged by the aforementioned art. 6 of the Legislative Decree on a basis of absolute uncertainty and in the total absence of objective reference criteria, de facto cancelling any effectiveness in relation to the desired prevention measures*" (Criminal Cassation, Section VI, 20 December 2013, no 3635).

Whilst waiting for jurisprudential findings which could help to clarify the application limits of the new case and in light of the indications contained in the aforementioned Memo no 19867 by CONFINDUSTRIA, it has been considered reasonable to draw up an Organizational Model which provides (in relation to the areas at risk of the crime of self-laundering being committed) deferred safeguards intended to prevent the crime of self-laundering and thus intended to avoid unlawful proceeds resulting from any malicious crime (even if not set down as an underlying crime presuming responsibility on the part of the entity) being used in the Company's business, economic or financial activities, whose circumvention is sanctioned by the Company's regulations.

These ad hoc safeguards are to be added, in the event the base crime should be also set down as an underlying crime presuming responsibility on the part of the entity, to the precautions already taken to prevent the source crime.

Given these comments, the following are examples of the crime cases referred to.

- Purchasing, receiving or hiding illegally-sourced money or items.
- The replacement or transfer of illegally-sourced money, goods or other utilities, or the execution, in relation to these, of other operations designed to hinder the identification of their illicit origin.
- Use of illegally-sourced money, goods or other utilities in economic or financial activities.
- Having committed or been complicit in committing a malicious crime, and using, replacing or transferring into economic, financial, business or speculative activities the money, goods or other

([6]) In particular, memo 19867 by CONFINDUSTRIA states that "*...positing the responsibility of the entity for all the crimes set down in our legal system, as base crimes to self-laundering, would mean overloading the prevention system set in place by the business concern, rendering its effect useless".*

utilities resulting from the commission of said crime in such a way as to actually hinder identification of their criminal origin.

2.13.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Gen. Dept. for Administration, Finance and Control
- Commercial Divisions/Departments
- Technical production departments

The **processes/sub-processes sensitive** to risk are as follows.

- Transactions involving the purchase and sale of financial instruments
- Transactions involving trading of products, goods or services
- Passive Cycle (purchases and supplies)/Management of invoices
- Active Cycle (sales)/Management of invoices
- Temporary Consortium Administrative Management/Management of economic relations between Partners
- Management of Buying-Selling Investments and Company Branches
- Management of Transactions with Related Parties
- Conferrals or contributions of capital into companies or other entities
- Intragroup transactions
- Real estate operations.

The following are the **methods for committing the crime** that can be theoretically hypothesized.

With reference to illegally-sourced money, goods or other utilities:

- purchase, receipt or concealment operations are carried out;
- irregular economic payments are made between partners in a Temporary Consortium;
- said assets are used in economic/financial operations;
- the assets are used in economic/financial operations in order to actually prevent identification of the fact that they are illegally sourced.

2.13.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.13.3.1 Specific principles of behavior

- In order to be fully assured that in the context of a supply to any Client, it is clear that the Company wishes to refrain from any corrupt behavior, or in any case illegal (even if carried out in the Company's interest or advantage), the company Parties mandated to authorize said supply, including for aspects connected to "passive cycle" phases (such as, for example, outsourcing aimed at providing the supply), must sign a declaration which certifies:
  - that, on the basis of the information at their disposal and up to the date of signing the declaration in question, at no stage of the commercial negotiations or contractual formalization, have any

episodes occurred which, even hypothetically, may be indirectly or directly attributed to the RELEVANT acts laid down in L. Decree 231/01;
- the undertaking to immediately report to the Supervisory Board pursuant to L. Decree 231/01 any attempts, episodes or acts, even hypothetically classifiable among the crimes mentioned above, should these occur after signing said declaration, until the supply has been fully implemented.

- In the event of supplies made to the Principal by a Temporary Consortium that an Engineering Group company takes part in, it is severely forbidden to implement any tacit economic payments between the partners. Any economic payment, in whatever form, must be explicit, motivated and duly formalized.
- In order to minimize the risk of committing the offenses considered herein, referring in particular, to the crime of self-laundering, the Company:
  - condemns any behavior intended to use money, goods or other utilities from a criminal source in its own economic, financial, business or speculative activities;
  - pays attention that those working in areas judged to be at risk of the crime should respect the laws, regulations and behavioral procedures established in relation to the management of the financial, shares and real estate resources and intended to prevent any possible economic use of criminal proceeds;
  - envisages the obligation to report any “atypical” operation of use in the company’s economic, financial, business and speculative activities.

  The following indicate atypical operations which must be specifically assessed in order to guarantee legitimacy in respect of the aims of preventing the risk of money laundering:
  1) extraneous or inconsistent with the corporate purpose, with the activities or economic-financial profile of the company or of the group to which it belongs;
  2) the absence of adequate justification, from the view point of normal managerial and corporate activities, in respect of the extraordinary nature of the amount or the unusual means of its fulfilment;
  3) the presence of commercial counterparts operating in countries whose anti-money laundering regime is not equivalent to that of countries within the European Community.

  Where there are one or more atypical indicators, the following reporting procedures are provided:
  a) in the case of operations falling within the power of signature and expenditure limits of an individual Manager, he/she shall promptly inform the Chairperson of the Board of Directors and the Supervisory Board for the necessary checks;
  b) if the atypical operation falls within the competence of the Board of Directors, it shall forward the Agenda or the relevant resolution to the Supervisory Board for the same ends.

  The above reports must be formalized in appropriate evidence forms.
- Bearing in mind legislative developments concerning money laundering, the Company shall continuously provide adequate training on how to correctly identify atypicality features to those responsible for economic, financial, business or speculative operations who are involved in the areas at risk.

2.13.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
11 – 01	A specific procedure, approved by the Board of Directors of the Parent Company, sets specific standards to be met in the process of identification, approval and execution of *Transactions with Related Parties*, such as to ensure the procedural and substantive transparency and fairness of these transactions, whether carried out directly or through Subsidiary Companies. The Procedure also applies, where applicable, to Transactions with Related Parties which include Subsidiaries, controlled directly or indirectly by the Parent Company. The Board of Directors of the latter examines in advance such operations. To this end, the Company's subsidiaries shall promptly inform the Parent Company of Transactions with Related Parties that they intend to approve, providing the necessary information and documentation in order to implement the provisions of the above-mentioned procedure.	**- PROCEDURE FOR DETECTING AND IMPLEMENTING TRANSACTIONS WITH RELATED PARTIES**
11 – 02	In order to minimize the risk of committing the crimes considered herein, it is mandatory to fully comply with all corporate rules applicable to *sensitive processes*, included in the procedures listed below: → Supplier Data Management: qualification and census for new Suppliers/amendment of personal and bank details → Qualified Supplier Register Management: selection of Suppliers from the Register, evaluation of qualified Suppliers and update of the Register → Passive Cycle Management: expense authorization, contract analysis and signature, management of invoices payable and payment mandates → Active Cycle Management: verification and authorization of cost-revenue budgets, contract analysis and signature, accrual of costs-revenues, management of invoices receivable → Client Data Management: census of new Clients/editing of personal data → Purchase/Sale of Acquisitions and Company Branches Management The rule which prohibits a sole person from enabling, managing, approving and closing a sensitive process must be respected. In particular, the authorization processes – both for purchase and sales contracts - must as a necessity formally involve at least two different Managers. Both types of contract must be signed by someone assigned the appropriate power of attorney, as documented in the system of Proxies, which is managed under central control. The table containing the names of Managers holding power for authorizing purchase requests, a table which is used by the electronic procedure that manages the authorization cycle, must also be subject to central management control. A similar central management control must be adopted for the table containing the names of Managers who may authorize the issue of an Offer/ Contract of sale. Finally, there must always be transparency and an adequate standard of documentation when performing the above-mentioned processes.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- RS01P01 Contract Acquisition Management Procedure** **- RS02P01 Management of First Supplier Qualification Procedure** **- RS02P02 Supplier Management Procedure** **- PGA11 Purchase/Sale of Acquisitions and Company Branches Management**

2.14 Crimes relating to breach of copyright (Art. 25-novies of L. Decree 231/01)

2.14.1 Crimes referred to by L. Decree 231/01

Article 25-novies of the Decree specifically refers to the following crimes.

A) - Making a protected original work, or part thereof, available to the public, within a system of telematics networks

B) - Crimes referred to in the above paragraph which are committed on others' works, not intended for publication or by usurping the authorship of the work...

C) – Unauthorized duplication, for profit,... of computer programs or, for the same purpose: the import, distribution, sale or possession for commercial or entrepreneurial purposes... of any means designed to remove or facilitate the removal... of systems used for protecting a computer program... or also: ... reproduction, transfer, distribution,... public presentation..., sale or lease of the contents of a database

D) – Unauthorized reproduction, transmission or dissemination in public, by any process,... of works or parts of literary works... or multimedia works... or databases...

E) - Failure to inform the SIAE of identification data for media not subject to tagging or misrepresentation

F) Fraudulent production, sale, installation..... of devices... designed to decode audio-visual transmissions under conditional access…

The description already given of the various crimes mentioned seems to provide a sufficient number of examples of the various crime cases.

2.14.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Commercial Divisions/Departments
- Technical production departments.

It is not thought possible to highlight specific **processes/sub-processes** more **sensitive** than others to the risk of the occurrence of the crimes under consideration herein.

The methods for committing the crime.

In relation to the crimes listed above, referred to under points E) and F): the occurrence of these crimes is not even theoretically conceivable within the corporate entity.

As regards at least one of the crime cases listed from points A) to D) inclusive, it can be theoretically hypothesized that the Company may experience one or both of the following situations:

- an original Third Party work is available, such as, purely by way of example: a computer program, a database, a technology solution, a document or a multimedia work;

or

- with reference to the copyright that may possibly be related to the original works mentioned above, devices are held which are designed solely for functionally removing devices put in place to protect those rights.

Under these circumstances, in order to obtain a profit and possibly upon prior removal of the protective devices originally prepared, the Company may (with reference to the abovementioned original works):

- make a protected original work (or part thereof) available, on telematics networks, usurping the authorship of the work,

or could

- illegally duplicate, reproduce, transfer, distribute, publicly disseminate, sell or rent an original work.

2.14.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.14.3.1 General principles of behavior

Please refer to the "*General principles of behavior*" specified in paragraph 2.2.

2.14.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
12 - 01	The following behaviors are expressly prohibited as they are prejudicial to copyright: - the receipt, distribution or use of software when such acts are contrary to the expressed will of the rightful owner; - the possession or use of software designed to circumvent or to break the software copy protection systems; - any operation aimed at compromising the data integrity, functionality or performance of IT systems; - any operation designed to circumvent or break control systems or IT systems; - any other use not permitted by the applicable legislation.	**- PGA02 Passive Cycle Management** **- RGP01 Regulation for company asset utilization**

2.15 Inducement not to make statements or to make fraudulent statements before the judicial authority (Art. 25-decies of L. Decree 231/01)

2.15.1 Crimes referred to by L. Decree 231/01

Article 25-decies of the Decree specifically refers to the following crime: *Inducement not to make statements or to make fraudulent statements to the judicial authority*.

A simple example of a crime case is the following: using violence, threats, offers or promises of money or other benefits to induce a person not to make statements to the judicial authority or to make false declarations.

2.15.2 Corporate contextualization and the methods for committing the crime

In relation to the presumed crime referred to herein, the Company's risk exposure is general in the sense that it is not considered possible to indicate **Parties/OUs** that are particularly **sensitive**:

The same applies to the identification of **sensitive processes/sub-processes**.

The methods for committing the crime: in the expectation of obtaining an illegal benefit for the Company, through the use of threats or promises, a person summoned to make statements in front of a judicial authority is induced not to make such statements or to make false ones.

2.15.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.15.3.1 Specific principles of behavior

It is absolutely forbidden, for anyone acting in the name of or on behalf of the Company, to bring about, be involved in or give rise to any behavior which amounts to committing this crime.

In more detailed terms, it is essential:

- that all activities and operations carried out on behalf of the Company should be guided by the utmost respect for the laws in force and the principles of fairness and transparency;
- that any behavior aiming at or resulting in inducing a third party to make false declarations in a criminal procedure is avoided;
- that a clear, transparent, diligent and cooperative demeanor is maintained with the Public Authorities, in particular with regard to the Judicial and Investigative Authorities, through the disclosure of all the information, data and news that may be requested.

2.16 Environmental crimes (Art. 25-undecies of L. Decree 231/01)

2.16.1 Crimes referred to by L. Decree 231/01

Article 25 undecies of the Decree, amended by Law no 68/15, specifically refers to “Environmental crimes". More precisely, it envisages a series of fines for an Entity in relation to the perpetration of lengthy series of crimes. The following is a *non-exhaustive* list of referenced crimes:

- Art. 452–bis of the Criminal Code: environmental pollution;
- art. 452–quater of the Criminal Code: environmental disaster;
- art. 452–quinquies of the Criminal Code: environmental disaster committed involuntarily;
- art. 452–octies of the Criminal Code: criminal and mafia-type association with the objective of committing any one of the crimes set forth in the new Title VI-bis of the Criminal Code;
- art. 452–sexies of the Criminal Code: trafficking in and abandonment of highly radioactive materials;
- Art. 452-quaterdecies of the Criminal Code: Organized activities for the illegal trafficking of waste;
- art. 727-bis of the Penal Code: killing, destroying, catching, taking, possessing specimens of protected wild fauna or flora;
- art. 733-bis of the Criminal Code: destruction or deterioration of habitat within a protected site.

With reference to the crimes laid down by art. 452-bis and 452-quarter of the Criminal Code, art. 25-undecies of L. Decree 231/01 (as amended by Law No 68/2015) provides that in the event of a conviction, in addition to the pecuniary sanctions laid down therein, the prohibition measures referred to in art 9 of the L. Decree itself should be applied to the Entity (for a period not exceeding one year in the event of conviction for the crime referred to in Article 452-bis of the Italian Criminal Code).

- With reference to L. Decree 152/06:
  - art. 137: discharge of industrial wastewater containing dangerous substances; discharge in the soil, subsoil and groundwater, discharge in sea waters by vessels or aircraft;
  - art. 256: management of waste without a permit;
  - art. 257: pollution of soil, subsoil, surface water or groundwater;
  - art. 258: violation of reporting requirements, record keeping requirements and forms;
  - art. 259: illegal waste trafficking;
  - art. 260-bis: false indications on the nature, composition and physical-chemical characteristics of waste; when providing a waste analysis certificate; entering a false waste analysis certificate in the

SISTRI register; omission or fraudulent alteration of the printed copy of the SISTRI waste handling form;

- art. 279, paragraph 5: harmful atmospheric emissions.

- Crimes provided for or referred to in Articles 1, paragraphs 1 and 2, 2, paragraphs 1 and 2, 3-bis paragraphs 1 and 6, and paragraph 4 of Law 150/92: import, export, possession, use for profit, purchase, sale, exhibition, or possession for sale or for commercial purposes of protected species.
- With reference to Law 549/93, Art. 3, paragraph 6: use of substances affecting the ozone layer and the environment.
- With reference to L. Decree 202/07:
  - art. 8, paragraphs 1 and 2: intentional pollution of seawater;
  - art. 9, paragraphs 1 and 2: negligent pollution of seawater.

2.16.2 Corporate contextualization and the methods for committing the crime

Compared with the many underlying crimes referred to herein, the risk exposure of the Company is limited to the disposal of industrial waste consisting of hardware equipment (or parts of equipment) that have reached the end of their life cycle or are exhausted (e.g., video screens, fax machines, toner cartridges, etc.);

As regards **Parties/OUs** particularly **sensitive** to the type of crimes considered, they are identified:

- within the Purchasing and General Affairs Department: those who deal with the procurement of hardware equipment for production and consumption and with the acquisition of maintenance services;
- the Manager responsible for monitoring the proper management of the waste produced in the various locations (known as "*Capo Palazzo (Office Chief)*").

Finally, as regards the identification of the **sensitive processes/subprocesses**, given the above, reference should be made to the procurement processes of the Passive Cycle, in particular to the acquisition of maintenance services relating to equipment and infrastructures.

The methods for committing the crime: in order to avoid the related costs, when carrying out its waste disposal activities, the Company fails to comply with the legislation to be applied in relation to the various types of crimes considered here.

2.16.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.16.3.1 Specific principles of behavior

Please refer to the "*General principles of behavior"* specified in paragraph 2.2.

2.16.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
13 – 01	All contracts concerning the provision of maintenance services which may produce waste (building material, electrical equipment, waste for equipment maintenance such as toners, etc.) must state that the supplier is expressly responsible for removing said material and that this must be carried out at the end of each working day.	**- PGA02 Passive Cycle Management** **- LGE01_PGE08Guidelines for Waste Management**
13 – 02	As far as the rules to be followed for managing printer cartridges (toner) are concerned, refer to the specifications in the reference Guidelines.	**- LGE01_PGE08 Guidelines for Waste Management**
13 - 03	As far as the rules to be followed for the disposal / scrapping of electrical and electronic equipment are concerned, refer to the specifications in the reference Guidelines.	**- LGA01 Guidelines for Disposal of Assets**

2.17 Employment of third-country nationals whose stay is illegal (Art. 25-duodecies of the L. Decree 231/01)

2.17.1 Crimes referred to by L. Decree 231/01

Article 25-duodecies of the Decree contextualizes the crime considered herein (pursuant to art. 22, paragraph 12-bis of L. Decree no. 286/1998) as follows:

an Employer takes on a foreign worker (non-European)

- without a residence permit
- whose permit has expired and the renewal of which has not been applied for in accordance with law
- whose permit is revoked or annulled

and, in any of the three cases mentioned above, any one of the following situations occurs:

- the employed workers are more than three in number;
- the employed workers are minors of non-working age;
- the employed workers are subjected to particularly exploitative working conditions referred to in paragraph 3 of art. 603-bis of the Penal Code (violation of the rules of safety and hygiene in the workplace, such as to expose the worker to health, safety or personal safety danger).

Following the changes made by Law 17 October 2017, n. 161, the criminal liability of the entity also extends to the crimes referred to in art. 12, paragraphs 3, 3-bis, 3-ter and 5 of the aforementioned L. Decree no. 286/1998 which punish:

- the activities of promoting, directing, organizing, financing transporting foreigners into the territory of the State or any other act aimed at illegally procuring their entry into the territory of the State, or of another State of which the person is not a citizen or does not have the right to a permanent residence permit in the event that:

a) the offense involves the entry or unlawful residence of five or more individuals within the territory of the State;

b) the individual's life or safety is placed at risk in order to obtain entry or unlawful residence;

c) the individual is subjected to inhumane or degrading treatment in order to obtain entry or unlawful residence;

d) the offense is committed by three or more individuals cooperating together, or using international transport services, or counterfeited or altered documents, or documents otherwise illegally obtained;

e) the individuals who have committed the offense have weapons or explosive materials at their disposal (art. 12, paragraph 3)[7].

- the conduct of those who, in order to obtain an unfair profit from the illegal status of the foreigner or in the context of the activities punished according to this article, encourage the continued stay of said individuals in the State's territory in violation of the provisions of L. Decree no. 286/1998 (Article 5 of Legislative Decree No. 286/1998).

2.17.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Gen. Dept. for Human Resources & Organization
- Gen. Dept. for Administration, Finance and Control (IT Consultancy Purchasing Department)

The **processes/sub-processes sensitive** to risk are as follows.

- Selection and recruitment of staff (employed or para-subordinate)
- Acquiring the provision of self-employment activity
- Management, over time, of the relationship with an Employee or a Self-employed person.

The methods for committing the crime: in order to achieve an economic advantage (such as, for example, paying a fee lower than the market, with equal skills), the Company uses non-EU personnel who do not comply with the regulations for residence on the national territory.

2.17.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.17.3.1 Specific principles of behavior

- In the context of acquiring a provision by a Self-employed person, should this be a person from outside the EU, a copy of a regular and valid Residence Permit issued to the Worker by the competent

[7] In accordance with art. 3-bis of L. Decree no. 286/1998 "*if two or more of the conditions indicated in sub-paragraphs a), b), c), d) and e) of paragraph 3 apply to the offenses committed, the penalty indicated therein shall be increased*". Pursuant to paragraph 3-ter of the same L. Decree no. 286/1998 "*The period of imprisonment is increased between one third and a half and a fine of Euro 25,000 is applied for each person if the facts referred to in paragraphs 1 and 3: a) are carried out in order to channel persons into prostitution or in any case for purposes of sexual or labor exploitation, or if they relate to the entry of minors to be employed in illegal activities in order to favor their exploitation; b) they are committed for the purpose of making a profit, even indirectly*".

authorities must be acquired, prior to finalizing the contractual relationship. In addition, before finalizing the contractual relationship, a signed declaration must be obtained from the worker, with which he/she undertakes: - to promptly notify the Company of any change in the status of the Residence Permit (expiration, renewal, suspension or revocation); - in the case of renewal, to provide a copy of the new Permit issued.

2.17.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
14 - 01	In the process of selection/recruitment of personnel, whether this is a candidate for an "internship" position or a person applying for a subordinate or para-subordinate position, when this concerns a non-EU Candidate, a copy of a regular and valid *Residence Permit* issued to the Applicant by the competent authorities must be acquired prior to finalizing the contractual relationship. In addition, before finalizing the contractual relationship, a signed declaration must be obtained from the worker, with which he/she undertakes: - to promptly notify the Company of any change in the status of the *Residence Permit* (expiration, renewal, suspension or revocation); - in the case of renewal, to provide a copy of the new *Permit* issued. Throughout the duration of the contract, the Personnel Administration Department verifies the continued validity of the permit and when its expiration date approaches – should the contract still be in place – warns the Collaborator of the need for renewal.	**- PGP09 Human Resources Management**

2.18 Tax offenses (Article 25-quinquiesdecies of L. Decree no. 231/2001)

2.18.1 Crimes referred to by L. Decree 231/01

Art. 25-quinquiesdecies, paragraph 1, of the Decree, introduced with L. Decree 26 October 2019, no. 124 (so-called "Tax decree"), converted, with amendments, with Law no 157 dated 19 December 2019, containing "*Urgent provisions on tax matters and for unavoidable needs*", specifically refers to some types of tax offenses envisaged by L. Decree no. 74/2000; in particular:

- art. 2, paragraphs 1 and 2-bis of L. Decree 74/2000: False statement by means of invoices or other documents for non-existent transactions;
- art. 3 L. Decree 74/2000: False statement by other means;
- art. 8, paragraphs 1 and 2-bis of L. Decree 74/2000: Issue of invoices or other documents for non-existent transactions;
- art. 10 L. Decree 74/2000: Concealment or destruction of accounting documents;
- art. 11 L. Decree 74/2000: Fraudulent evasion of tax payments.

L. Decree July 14. 2020, n. 75, transposing Directive EU/2017/1371 (so-called "PIF Directive"), relating to the "*fight against fraud which damages the Union's financial interests by means of criminal law*", has further expanded, through the introduction in Decree 231 of paragraph 1-bis of art. 25-quinquiesdecies, the category of tax-based crimes.

Specifically, starting from conduct committed from 30 July 2020, the following crimes are relevant for the purposes of the entity's liability, if committed in the context of cross-border fraudulent systems (within the European Union) as well as for the purpose of evading the tax on added value for a total amount of not less than 10 million euro:

- art. 4 L. Decree 74/2000: Unfaithful tax declaration;
- art. 5, L. Decree 74/2000: Omitted tax declaration;
- art. 10-quater of L. Decree 74/2000: Undue compensation.

The following are examples of the crime cases referred to.

A) Signing fictitious agreements or contracts and the consequent use, for tax declaration purposes and in order to evade taxes, of invoices or other documents issued in relation to transactions not actually carried out - in whole or in part - and subsequently recorded in the mandatory accounting records or held to be used with evidentiary purposes towards the financial administration (Article 2 of L. Decree 74/2000);

B) the use of false documents, other than the typical tax-related ones referred to in art. 2 L. Decree 74/2000, for tax declaration purposes and to reduce taxes by hindering the financial administration's assessment activity, or the alteration of the data referred to in the mandatory accounting records with fraudulent methods (Article 3 of L. Decree 74/2000);

C) the issue of invoices or other documents for transactions not carried out - in whole or in part - in order to allow a third party, in the context of an agreement with mutual economic advantages, to evade income or added value taxes (Article 8 of L. Decree 74/2000);

D) the concealment of material or the destruction - in whole or in part - of accounting records or documents which must be kept, in such a way as not to allow the reconstruction of the income or in order to remove evidence of the incorrect keeping of the accounting records and thus to evade income or value added taxes (Article 10 of L. Decree 74/2000);

E) the disposal of an asset through an expression of will which does not correspond to the real intention of the parties or the performance of other acts (such as, by way of example and not limited to, a simulated sale or a fraudulent establishment of a trust fund or of a merely apparent trust) of their own or others' assets in order to make the compulsory collection procedure totally or partially ineffective (Article 11 of L. Decree 74/2000);

F) carrying out an underestimation of revenues or an overestimation of costs concerning the entry of active elements for an amount lower than the actual one or of non-existent passive elements (Article 4 of L. Decree 74/2000);

G) the correct compilation of the income-tax return and its transmission beyond 90 days from the deadline (Article 5 of L. Decree 74/2000);

H) the submission of the F24 form indicating credits which are not due or are non-existent, in order to pay less taxes than those due (art. 10-quater L. Decree 74/2000).

2.18.2 Corporate contextualization and the methods for committing the crime

As concerns the abovementioned underlying tax offenses, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- General Department for Financial Administration and Control;
- Sales Specialists;
- Clients & Project Management:
- Cloud & Technology Services:
- General Department for Human Resources & Organization;

*Business & User Services***:**

In addition, the risk exposure also concerns the following sensitive Parties/OUs:

- Purchasing and General Affairs Department;
- Technical production departments;
- Commercial Divisions/Departments;
- Internal Information Systems Department;
- all OUs operating in the accounting and tax fields;
- all OUs operating in the technical and commercial fields.

The **risk-sensitive processes/sub-processes**, transversally to all the aforementioned offenses, by way of example and not limited to, refer to:

- Management of accounting closing entries
- Management of the Balance Sheet
- Management of tax obligations
- Management of Financial Services and Treasury/Management of Bank Transactions and Financial Flows

2.18.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.18.3.1 Specific principles of behavior

The Parties mentioned above, as well as all the Recipients of this Model, are required to scrupulously comply with all the regulations in force.

In particular, it is expressly forbidden to:

- instigate, collaborate in or contribute to causing acts or conduct which, taken directly or indirectly, involve the offenses included among those considered above;
- violate the principles and rules that are provided for in this Special Section and in the Code of Ethics;
- indicate false, artificial, incomplete or otherwise not true data for the processing or entry of tax document data;
- prepare false documentation, suitable for providing a false accounting representation of the taxpayer's tax situation;
- create invoices or other documents for non-existent transactions;
- use and record invoices or other documents for non-existent transactions in the mandatory accounting records;
- hold invoices or other documents for non-existent transactions to be used for evidentiary purposes in relations with the Financial Administration;
- enter into de facto agreements other than those laid down in the relative contract, in order to disguise the actual contractor;
- allocate fees or services to external parties (e.g. consultants, auditors or other professionals) which are not justified by any type of assignment, as well as pay fees for services which have not been performed;
- carry out sales transactions or any other fraudulent transaction aimed at evading the payment by Engineering of income taxes and value added tax or of interest or administrative penalties relating to such taxes.

2.18.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
15 - 01	The rule, provided for in all the procedures mentioned, which prohibits a sole person from enabling, managing, approving and closing a sensitive process must be respected. In order to minimize the risk of committing the crimes considered herein, the Cost Support process expressly provides for the segregation of duties, involving multiple sensitive Parties and/or OUs (Requesting Body, Centralized Purchasing Offices, Supplier Accounting Service). In any case, the process takes place with the support of IT platforms which perform automated checks: → SAP: support for the General and Analytical Accounting Management; → SIIWEB: support for the issue/approval of PRs and POs; → PAGE: supplier portal for the census and management of the Qualified Suppliers List.	**- PGA02 Passive Cycle Management** **- PGA04 Supply Quote Management** **- PGA05 Cash Management** **- RS02P02 Supplier Management Procedure** **- PGA08 Account Closure Management** **- PGA06 Financial and Treasury Services Management** **- PGA14 Management of Proxies and Powers of Attorney**
15 - 02	In order to proceed with issuing an active invoice, a contractual file must exist, whose development process must respect the principle of segregation of duties, involving multiple sensitive Parties and/or OUs: → Commercial Structure: responsible for formalizing and implementing contracts; → Contracts Offices: responsible for managing the archiving of the documents and for verifying the correctness/completeness of the documents making up the contractual file; → Administrative Department: responsible for the administrative management of the contract and the client. In any case, the process takes place with the support of IT platforms which perform automated checks: → SAP: support for the General and Analytical Accounting Management; → Sial: support for managing orders with the inclusion of billing plans for issuing/approving invoices to clients; → OrMe – Order Management of Engineering: an application which allows the management of the entire negotiation, from the *prospect* to formalizing the contract.	**PGA03 Active Cycle Management** **- PGA13 Consortium/Temporary grouping Administrative Management** **- PGA08 Account Closure Management** **- PGA06 Financial and Treasury Services Management** **- PGA14 Management of Proxies and Powers of Attorney**

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
15 - 03	In the process of managing accounting records and preparing tax forms, the documentation relating to contracts with both suppliers and clients must be kept, both in paper format and in electronic format (PDFs), respectively at the Centralized Purchasing Office and at the Contracts Office. The registration and storage of tax documents for suppliers and customers must be kept by the Supplier Accounting Office and by the Active Cycle Service, respectively, without prejudice to the introduction of the additional IT systems supporting the storage of the documentation, managed by the Revenue Agency, following the entry into force of the "electronic invoice" legislation. The IT applications which regulate and control access to company systems must be managed centrally, in full compliance with strict criteria for defining responsibilities, separating functions and limiting access to those data that are essential as well as strictly necessary. Tax and/or accounting data are copied to external media (physical or virtual) in order to allow their recovery if required, by means of the "Restore" reverse operation; the data is restored both in the most recent version and in an earlier version should unauthorized interventions on the accounting data be ascertained.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- PGA08 Account Closure Management** **- PGP03 Management of Access to Business Systems** **- RS08PR08 Backup Management Procedure**
15 - 04	In the process of managing company assets, only those Parties expressly authorized through a formal conferral of powers by virtue of their specific position within the company organization, may act in the name and on behalf of Engineering; powers of attorney and proxies must comply with the indicated limits.	**- LGA01 Guidelines for Disposal of Assets** **- PGA14 Management of Proxies and Powers of Attorney**

2.19 Transnational crimes - Inducing false witness - Aiding and abetting (Article 10, paragraph 9, of Law 146/06)

2.19.1 Crimes referred to by L. Decree 231/01

Article 10 of law 146/06, in relation to committing the crimes referred to in Articles 377 and 378-bis of the Penal Code, recalls the Entity's administrative liability and the application of the sanctions laid down by Legislative Decree 231/01; this particularly applies to the following "*transnational*" crimes:

- Inducement not to make statements or to make fraudulent statements before the judicial authority
- Aiding and abetting

As concerns the crime of "*Inducement not to make statements or to make fraudulent statements before the judicial authority*", please refer to the same offense when discussed with reference to Art. 24-decies of L. Decree 231/01.

It should be noted that art. 3 of the aforementioned Law n. 146/06 defines a crime as "*transnational*" when it involves an organized criminal group and:

- the crime occurs in more than one State
- or it occurs in one State, but a substantial part of its preparation, planning, management or control takes place in another State
- or it occurs in one State, but involves an organized criminal group engaged in criminal activities in more than one State
- or it occurs in one State but has substantial effects in another State.

This is an example of the second crime case considered herein (with reference to the circumstances referred to by the term "transnational crime"): after committing a crime for which the penalty by law is a life sentence or imprisonment, help is given to an individual to evade the investigations of the authorities, or to evade efforts to impose this penalty.

2.19.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, no **particularly sensitive Parties/OUs or processes** can be highlighted.

The following are the **methods for committing the crime** that can be theoretically hypothesized.

In purely general terms, in personal relations with Employees or Third Parties: adopting a behavior that does not comply with the principles of legality, integrity and transparency.

2.19.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.19.3.1 Specific principles of behavior

As concerns the "*Inducement not to make statements or to make fraudulent statements before the judicial authorities*" crime, please refer to the same offense when discussed with reference to Art. 24-decies of L. Decree 231/01.

It is absolutely forbidden in any case, for anyone acting in the name of or on behalf of the Company, to bring about, be involved in or give rise to any behavior which amounts to committing one of these crimes. In more detailed terms, it is essential:

- that all activities and operations carried out on behalf of the Company should be guided by the utmost respect for the laws in force and the principles of fairness and transparency;
- that a clear, transparent, diligent and cooperative demeanor is maintained with the Public Authorities, in particular with regard to the Judicial and Investigative Authorities, through the disclosure of all the information, data and news that may be requested.

2.20 Transnational crimes – Criminal and mafia-type association (Art. 10 paragraph 2 of Law 146/06)

2.20.1 Crimes referred to by L. Decree 231/01

Article 10 of law 146/06, in relation to committing the crimes referred to in Articles 416 and 416-bis of the Penal Code, recalls the Entity's administrative liability and the application of the sanctions laid down by L. Decree 231/01; this particularly applies to the following "*transnational*" crimes:

- Criminal associations
- Mafia-type organizations

As concerns the concept of "*transnational crime*", please refer to the corresponding paragraph above concerning the first of the *transnational crimes* illustrated.

With reference to the crimes mentioned, the comments made in the "Organized crime crimes" section are applied here (Art. 24-ter of Legislative Decree 231/01).

2.20.2 Corporate contextualization and the methods for committing the crime

With reference to the crimes mentioned, the comments made in the "Organized crime crimes" section are applied here (Art. 24-ter of Legislative Decree 231/01).

2.20.3 Corporate protocols defending against risk

With reference to the crimes mentioned, the comments made in the "Organized crime crimes" section are applied here (Art. 24-ter of Legislative Decree 231/01).

2.21 Transnational crimes - Criminal association, tobacco smuggling (Art. 10, paragraph 2, of Law 146/06)

2.21.1 Crimes referred to by L. Decree 231/01

Article 10 of Law 146/06, in relation to committing the crimes referred to in Art 291-quater of Presidential Decree no 43/73, recalls the Entity's administrative liability and the application of the sanctions laid down by L. Decree 231/01; this particularly applies to the following "*transnational*" crime:

- Criminal association for tobacco smuggling

As concerns the concept of "*transnational crime*", please refer to the corresponding paragraph above concerning the first of the *transnational crimes* illustrated.

The following are examples of the crime cases referred to.

With reference to the circumstances referred to by the term "*transnational crime*" and, specifically, to crimes involving the introduction, transportation, sale, purchase or possession within the State of contraband tobacco manufactured abroad:

- three or more people conspiring to commit several crimes
- an association similar to the one mentioned above is promoted, directed, organized or funded
- becoming a member of an association like the one referred to above.

2.21.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Senior Management
- Gen. Dept. for Administration, Finance and Control
- Commercial Divisions/Departments

The **processes/sub-processes sensitive** to risk are generally the following:

- Passive Cycle (purchases and supplies)
- Active Cycle (sales).

The following are the **methods for committing the crime** that can be theoretically hypothesized.

In general terms: establishing and maintaining business, economic or commercial relationships of a criminal nature with the organization of a Client, Supplier or Partner.

2.21.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.21.3.1 Specific principles of behavior

It is absolutely forbidden, for anyone acting in the name of or on behalf of the Company, to bring about, be involved in or give rise to any behavior which amounts to committing one of these crimes. In more detailed terms, it is essential:

- that all activities and operations carried out on behalf of the Company should be guided by the utmost respect for the laws in force and the principles of fairness and transparency;
- that compliance with the legislation in force, as well as with the corporate procedures and protocols, be guaranteed, in relation to both the active and passive Cycles and to the management and use of resources and business assets, particularly for those which originate from outside Italy.

2.21.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
	.	
15 – 01	In order to minimize the risk of committing the crimes considered herein, it is mandatory to fully comply with all corporate rules applicable to *sensitive processes*, included in the procedures listed below: → Supplier Data Management: qualification and census for new Suppliers/amendment of personal and bank details → Qualified Supplier Register Management: selection of Suppliers from the Register, evaluation of qualified Suppliers and update of the Register → Passive Cycle Management: expense authorization, contract analysis and signature, management of invoices payable and payment mandates → Active Cycle Management: verification and authorization of cost-revenue budgets, contract analysis and signature, accrual of costs-revenues, management of invoices receivable → Client Data Management: census of new Clients/editing of personal data The rule which prohibits a sole person from enabling, managing, approving and closing a sensitive process must be respected. In particular, the authorization processes – both for purchase and sales contracts - must as a necessity formally involve at least two different Managers. Both types of contract must be signed by someone assigned the appropriate power of attorney, as documented in the system of Proxies, which is managed under central control. The table containing the names of Managers holding power for authorizing purchase requests, a table which is used by the electronic procedure that manages the authorization cycle, must also be subject to central management control. A similar central management control must be adopted for the table containing the names of Managers who may authorize the issue of an Offer/ Contract of sale. Finally, there must always be transparency and an adequate standard of documentation when performing the above-mentioned processes.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- RS01P01 Contract Acquisition Management Procedure** **- RS02P01 Management of First Supplier Qualification Procedure** **- RS02P02 Supplier Management Procedure**

2.22 Transnational crimes – Conspiracy to traffic in drugs (Art. 10, paragraph 2, of Law 146/06)

2.22.1 Crimes referred to by L. Decree 231/01

Article 10 of Law 146/06, in relation to perpetrating the crimes referred to in Art 74 of Presidential Decree no 309/90, recalls the Entity's administrative liability and the application of the sanctions laid down by L. Decree 231/01; this particularly applies to the following "*transnational*" crime:

- Organization dedicated to illicitly trafficking in drugs or psychotropic substances

As concerns the concept of "*transnational crime*", please refer to the corresponding paragraph above concerning the first of the *transnational crimes* illustrated.

With reference to the crime mentioned, the comments made in the "Organized crime crimes" section are applied here. (Art. 24-ter of Legislative Decree 231/01).

2.22.2 Corporate contextualization and the methods for committing the crime

With reference to the crime mentioned, the comments made in the "Organized crime crimes" section are applied here. (Art. 24-ter of Legislative Decree 231/01).

2.22.3 Corporate protocols defending against risk

With reference to the crime mentioned, the comments made in the "Organized crime crimes" section are applied here. (Art. 24-ter of Legislative Decree 231/01).

2.23 Transnational crimes – Illegal immigration (Art. 10 paragraph 7 of Law 146/06)

2.23.1 Crimes referred to by L. Decree 231/01

Article 10 of Law 146/06, in relation to committing the crimes referred to in Art. 12 (paragraphs: 3, 3-bis, 3-ter, 5) of L. Decree no 286/98, recalls the Entity's administrative liability and the application of the sanctions laid down by L. Decree 231/01; this particularly applies to the following "*transnational*" crime:

- Illegal immigration

As concerns the concept of "*transnational crime*", please refer to the corresponding paragraph above concerning the first of the *transnational crimes* illustrated.

The following are examples of the crime cases referred to.

With reference to the circumstances referred to by the term "*transnational crimes*":

- with a view to obtaining a profit, even indirectly, engaging in acts aimed at obtaining the entry of a person into the territory of the State in violation of the law, or to obtain illegal entry into another State which the person is not a citizen of or where the individual in question is not entitled to permanent residence, potentially with the aim of channeling the person into prostitution or sexual exploitation...
- with a view to obtaining an unfair profit from the illegal status of a foreigner, encouraging the continued stay of such individuals in the State's territory, in violation of the law.

2.23.2 Corporate contextualization and the methods for committing the crime

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Senior Management
- Gen. Dept. for Administration, Finance and Control
- Commercial Divisions/Departments
- Gen. Dept. for Human Resources & Organization

The **processes/sub-processes sensitive** to risk are generally the following:

- Passive Cycle (purchases and supplies)
- Active Cycle (sales)
- Personnel Management (recruitment).

The **methods for committing the crime** that can be theoretically hypothesized are as follows.

- In relationships with individual persons: the adoption of a behavior which fails to comply with the principles of legality, fairness and transparency
- Establishing and maintaining business, economic or commercial relationships of a criminal nature with the organization of a Client, Supplier or Partner.

2.23.3 Corporate protocols defending against risk

The principles, rules of conduct, protocols and controls applied and the reference company documents are shown below.

2.23.3.1 Specific principles of behavior

It is absolutely forbidden, for anyone acting in the name of or on behalf of the Company, to bring about, be involved in or give rise to any behavior which amounts to committing one of these crimes. In more detailed terms, it is essential:

- that all activities and operations carried out on behalf of the Company should be guided by the utmost respect for the laws in force and the principles of fairness and transparency;
- that compliance with the legislation in force, as well as with the corporate procedures and protocols, be guaranteed, in relation to both the active and passive Cycles and to the management and use of resources and business assets, particularly for those which originate from outside Italy;
- that compliance with the legislation in force on immigration and labor, particularly with reference to aspects associated with the establishment of working relationships, be guaranteed.

2.23.3.2 Specific protocols and controls relating to corporate processes

Prot. Id.	Prescribed corporate behavior, protocols and controls applied	Name of corporate reference document
16 - 01	In order to minimize the risk of committing the crimes considered herein, it is mandatory to fully comply with all corporate rules applicable to *sensitive processes*, included in the procedures listed below: → Supplier Data Management: qualification and census for new Suppliers/amendment of personal and bank details → Qualified Supplier Register Management: selection of Suppliers from the Register, evaluation of qualified Suppliers and update of the Register → Passive Cycle Management: expense authorization, contract analysis and signature, management of invoices payable and payment mandates → Active Cycle Management: verification and authorization of cost-revenue budgets, contract analysis and signature, accrual of costs-revenues, management of invoices receivable → Client Data Management: census of new Clients/editing of personal data → Human Resources Management/Recruitment of staff The rule which prohibits a sole person from enabling, managing, approving and closing a sensitive process must be respected. In particular, the authorization processes – both for purchase and sales contracts - must as a necessity formally involve at least two different Managers. Both types of contract must be signed by someone assigned the appropriate power of attorney, as documented in the system of Proxies, which is managed under central control. The table containing the names of Managers holding power for authorizing purchase requests, a table which is used by the electronic procedure that manages the authorization cycle, must also be subject to central management control. A similar central management control must be adopted for the table containing the names of Managers who may authorize the issue of an Offer/ Contract of sale. Finally, there must always be transparency and an adequate standard of documentation when performing the above-mentioned processes.	**- PGA02 Passive Cycle Management** **- PGA03 Active Cycle Management** **- RS01P01 Contract Acquisition Management Procedure** **- RS02P01 Management of First Supplier Qualification Procedure** **- RS02P02 Supplier Management Procedure** **- PGP09 Human Resources Management**

2.24 Failure to comply with prohibition orders (art 23 L. Decree 231/01)

2.24.1 Crimes referred to by L. Decree 231/01

Pursuant to art. 23 of the Decree "*Anybody who, when carrying out the activity of the entity to which a sanction or a precautionary prohibitory measure has been applied, transgresses the obligations or prohibitions related to such sanctions or measures, is punished with imprisonment from six months to three years. 2. In the case referred to in point 1, a pecuniary administrative sanction between two hundred and six hundred quotas and the confiscation of the profit is applied to the entity in whose interest or advantage the crime was committed, in accordance with article 19*."
Pursuant to the third paragraph of the law in question, if the entity has made a significant profit from the offense described above, prohibitory measures are applied, including others than those previously imposed.

2.24.2 Corporate contextualization

As concerns the underlying crimes referred to herein, the Company's risk exposure relates to the following **sensitive Parties/OUs**:

- Governance Body
- Legal and Corporate Affairs Department
- Company functions that manage authorizations, licenses or concessions issued to the Company
- Company functions that have contacts with the Public Administration
- Company functions that manage incentives, loans, grants or contributions allocated to the Company
- Company functions that manage the advertising of goods or services.

2.24.3 Corporate protocols defending against risk

The following are the principles and rules of conduct that the Company agrees to comply with in order to avoid committing the offense within the company context.

2.24.3.1 Specific principles of behavior

It is absolutely forbidden, for anyone acting in the name of or on behalf of the Company, to bring about, be involved in or give rise to any behavior which amounts to committing this crime. In more detailed terms:

- it is essential that all activities and operations carried out on behalf of the Company should be guided by the utmost respect for the laws in force and the principles of fairness and transparency;
- a prompt communication (i.e. as quickly as possible) of the sanctions and/or precautionary prohibition measures applied to the Company, to the Company Functions responsible for the activities towards which the sanctions and measures were applied, as well as to the subjects involved in the same productive processes, in order that they may be immediately aware and, therefore, be able to act in compliance with the requirements imposed by the Judicial Authority, must be provided for;
- all activities and operations carried out within the company and/or on behalf of the Company must be based on compliance with the obligations and prohibitions inherent to the sanction or with the precautionary prohibition measure possibly imposed on the entity.