

FREE2MOVE ESOLUTIONS S.P.A.
***“ORGANIZATION, MANAGEMENT AND CONTROL MODEL
PURSUANT TO LEGISLATIVE DECREE 231/2001”***

INDEX

SECTION I - INTRODUCTION	7
1.1 Legislative Decree 231/2001 and relevant regulations	7
1.1.1 Predicate Offences	7
1.1.1 Criteria for attributing liability to Entities	8
1.1.2 Sanctions applicable to the Entity	10
1.1.3 Exemption of liability: the organization, management and control model pursuant to Decree	12
1.1.4 Offences committed abroad	13
1.2 The function of the Model according to the Decree	13
1.3 Reference Guidelines	14
SECTION II – THE COMPANY	15
2.1 Free2Move eSolutions S.p.A.....	15
2.2 The Ethics & Compliance of F2M eSolutions.....	15
2.3 The current organization of the Company	15
2.4 The Corporate Governance system	15
SECTION III – CONSTRUCTION OF THE MODEL.....	16
3.1 The F2M eSolutions	16
3.1.1 The Model’s inspiring principles and elements	16
3.1.2 The Model’s features	16
3.1.3 Method used to construct the Model	16
3.1.4 The Model’s structure	17
3.1.5 The Model’s Recipients	18
3.1.6 Adoption of the F2M eSolutions Model and subsequent amendments ...	18
3.1.7 Implementation of the F2M eSolutions Model.....	18
3.2 The Supervisory Body.....	19
3.2.1 Identification of the Supervisory Body: appointments and dismissals	19
3.2.2 Functions and powers of the Supervisory Body.....	21
3.2.3 Reporting by the Supervisory Board to top management	22
3.2.4 Information flows to the Supervisory Body.....	23
3.2.5 Information collection and storage	24
3.3 Whistleblowing system	24

3.4	<i>Checks on the adequacy of the Model</i>	24
SECTION IV - CIRCULATION OF THE MODEL		25
4.1	<i>Employee training and information</i>	25
4.2	<i>Information to Service Companies, Consultants and Partners</i>	26
4.3	<i>Information to Directors and Auditors</i>	26
SECTION V - DISCIPLINARY SYSTEM		27
5.1	<i>Function of the disciplinary system</i>	27
5.2	<i>Measures against middle managers, white collar and blue collar workers</i>	28
5.2.1	Disciplinary System	28
5.2.2	Model Violations and Sanctions	29
5.2.3	Measures against executives	30
5.2.4	Measures against employees subject to management or supervision	30
5.2.5	Measures against Directors	31
5.2.6	Measures against Auditors.....	31
5.2.7	Measures against Service Companies, Consultants and Partners.....	31
5.2.8	Measures against the Supervisory Body and other subjects	31
SECTION VI – THE MODEL		32
6.1	<i>General Control Environment</i>	32
6.1.1	The Company's organizational system	32
6.1.2	The delegation and proxy system	32
6.1.3	General principles of conduct.....	33
6.1.4	Specific control standards	35
6.1.5	Financial flow management system	36
6.2	<i>F2M eSolutions Sensitive Processes</i>	37
A.	<i>Sensitive Processes in criminal offenses against the Public Administration and against the Administration of Justice</i>	39
B.	<i>Sensitive Processes in cybercrime Offences</i>	43
C.	<i>Sensitive Processes in organized crime Offences</i>	45
D.	<i>Sensitive Processes within the context of Offences of falsification of instruments or signs of identification (counterfeiting, alteration or use of trademarks or distinctive signs or of patents, models and designs) and Offences against industry and commerce</i>	47
E.	<i>Sensitive Processes in corporate crimes</i>	50

F.	<i>Sensitive Processes in crimes of terrorism and subversion of the democratic order</i>	54
G.	<i>Sensitive Processes in Offences against the individual</i>	55
H.	<i>Sensitive Processes in market abuse Offences</i>	56
I.	<i>Sensitive Processes in crimes of manslaughter and serious or very serious culpable injuries (committed in breach of the regulations on health and safety in the workplace).....</i>	58
J.	<i>Sensitive Processes in crimes of receiving of stolen goods, money laundering and utilization of money, goods or benefits of unlawful origin, and self-laundering.....</i>	71
K.	<i>Sensitive Processes in Offences related to copyright infringement.....</i>	74
L.	<i>Sensitive Processes in environmental crimes</i>	77
M.	<i>Sensitive Processes in tax crimes</i>	84

DEFINITIONS

<u>At-Risk Activity</u>	A phase in a Sensitive Process which might present the premises/potential for the commission of a Predicate Offence
<u>Instrumental Activity</u>	An activity through which it is possible to commit corruption/malfeasance Offences
<u>CCNL Journalists</u>	National Collective Labour Agreement for professional journalists employed by publishers of newspapers and periodicals, press agencies and private radio and television broadcaster
<u>CCNL Metalworkers</u>	Metalworkers' industry first level National Collective Labour Agreement for workers in the private engineering sector and equipment installers (for non-executive Employees) currently in force and applied by F2M eSolutions
<u>Code of Ethics</u>	Code of Ethics adopted by F2M eSolutions
<u>Consultants</u>	Individuals acting in the name and/or on behalf of F2M eSolutions on the basis of an assignment or another type of collaboration, including term contracts
<u>Corporate Bodies</u>	Members of the F2M eSolutions Board of Directors and of the Board of Auditors
<u>Decree</u>	Legislative Decree no. 231 dated 8 June 2001 and subsequent amendments
<u>Employees</u>	All F2M eSolutions employees (executives included)
<u>Entity or Entities</u>	Entities with legal personality to which the provisions set out by the Decree apply
<u>Free2Move eSolutions S.p.A.</u>	Joint stock company, with headquarters in Piazzale Lodi 3, Milan, registered in the Milan Companies Register with number MI – 2605587 (hereinafter, "F2M eSolutions" or the "Company")
<u>Model</u>	The organization, management and control model pursuant to Decree adopted by the Company
<u>Offences _____ or Predicate Offences</u>	Criminal Offence/s that if committed entail administrative liability for the Entities and implementation of the rules envisaged by the Decree (including subsequent legislative additions and amendments)
<u>Partner</u>	Natural or legal person (temporary business associations - ATI, joint-ventures, consortia, etc.), with which F2M eSolutions agrees on a form of contractually regulated cooperation, <i>i.e.</i> F2M eSolutions' contractual

counterparty/parties, both natural and legal persons (e.g. suppliers, customers, agents, etc. ...) that are to cooperate on an ongoing basis with the Company within the sphere of Sensitive Processes

<u>Public Administration or P.A.</u>	Public Administration, including the relevant officials and persons responsible for public services
<u>Recipient</u>	Corporate Bodies, Employees, Service Companies, Consultants and Partners (including suppliers, customers and additional third parties that cooperate with F2M eSolutions in the area of Sensitive Processes)
<u>Reference Guidelines</u>	Guidelines per the construction of the organization, management and control model pursuant to Decree approved by Confindustria on 7 March 2002 and subsequent amendments and additions
<u>Sensitive Processes</u>	F2M eSolutions activities which present a risk in relation to the commission Predicate Offences
<u>Supervisory Body</u>	Body responsible for overseeing implementation of and compliance with the Model and its related updates

SECTION I - INTRODUCTION

1.1 Legislative Decree 231/2001 and relevant regulations

The Decree was issued on 8 June 2001 in execution of the delegated power pursuant to Article 11 of Law no. 300 dated 29 September 2000. It came into force the following July 4, adapting internal regulations concerning the liability of legal persons to several international agreements to which Italy had been a signatory for some time.

The Decree laying down “*Provisions on the administrative liability of legal persons, companies and associations, including those without legal personality*” has indeed for the first time introduced into the Italian legal system the administrative or “quasi-criminal” liability of Entities for Offences committed in their interest or to their benefit. In particular, the Decree envisages that Entities may be held liable and consequently sanctioned in relation to the commission of Offences it specifies in an exhaustive list (so-called Predicate Offences, see par. **Errore. L'origine riferimento non è stata trovata.** and **Errore. L'origine riferimento non è stata trovata.** below).

The provisions of the Decree identify as those who may commit a Predicate Offence individuals holding positions of representation, administration or management of the Entity or of any of its organizational units enjoying financial and functional autonomy, as well as individuals responsible, also de facto, for the management and control of the same (individuals in leadership positions) and, lastly, individuals subject to the direction or supervision of one of the above indicated subjects (parties subject to their direction and oversight). This liability is additional to that of the natural person who has materially committed the Offence (par. **Errore. L'origine riferimento non è stata trovata.**).

The Decree provides for sanctions to the assets of the entities that have benefitted from the committed Predicate Offences. A monetary sanction is envisaged for all Offences committed; in the more serious cases disqualifying measures are envisaged, such as the suspension or revocation of licences and concessions, the prohibition on contracting with the Public Administration, the prohibition on conducting business activities, denial or revocation of funding and subsidies, the prohibition on advertising goods and services (for an in-depth analysis of the sanctions envisaged by the Decree see par. **Errore. L'origine riferimento non è stata trovata.** below).

The Decree envisages a form of exemption from administrative liability that is applied if (i) the Entity proves it has adopted and effectively implemented, prior to the commission of the Offence, an appropriate Organization and Control Model suitable to prevent Offences of the kind that has occurred, tasking a body with autonomous powers of initiative and control (Supervisory Body) with monitoring the operation and observance of the model itself, (ii) the fact has been committed by fraudulently eluding the Model and (iii) the Supervisory Body's oversight was not omitted or insufficient.

1.1.1 Predicate Offences

The Offences, which when committed entail administrative liability for entities, are identified by the Decree in a strict and exhaustive list. Although the list may be amended and other Offences may be added to by the legislator, the following Predicate Offences currently provided for by the Decree are:

- a) Offences committed in relations with the Public Administration (articles 24 and 25 of the Decree);
- b) Cybercrimes and unlawful data processing (Article 24-*bis* of the Decree);
- c) Offences concerning counterfeiting currency, credit cards, tax stamps and distinguishing instruments or signs (Article 25-*bis* of the Decree);

- e) Offences against industry and commerce (Article 25-*bis*.1 of the Decree);
- f) Corporate crimes (Article 25-*ter* of the Decree);
- g) Offences committed for purposes of terrorism or subverting the democratic order (Article 25-*quater* of the Decree);
- h) Female genital mutilation practices (Article 25-*quater*.1 of the Decree);
- i) Offences against the person (Article 25-*quinquies* of the Decree);
- j) Market abuse Offences (Article 25-*sexies* of the Decree);
- k) Transnational Offences (Law no. 146 dated 16 March 2006,);
- l) Manslaughter and causing serious or very serious injury in breach of legal provisions governing the protection of health and safety at the workplace (Article 25-*septies* of the Decree);
- m) Receiving stolen goods, money laundering and the use of unlawfully obtained money, goods or benefits and self-laundering (Article 25-*octies* of the Decree);
- n) Copyright infringement Offences (Article 25-*novies* of the Decree);
- o) Inducing someone to withhold testimony or make false statements to the judicial authorities (Article 25-*decies* of the Decree);
- p) Environmental crimes (Article 25-*undecies* of the Decree);
- q) Employing third-country nationals without a residence permit (Article 25-*duodecies* of the Decree)
- r) Xenophobia and racism (Article 25-*terdecies* of the Decree);
- s) Fraud in sports competitions, illegally providing gaming, betting and gambling services using forbidden machines (Article 25-*quaterdecies* of the Decree);
- t) Tax Offences (Article 25-*quinquiesdecies* of the Decree);
- u) Contraband Offences (Article 25-*sexiesdecies* of the Decree);
- v) Failure to comply with disqualification sanctions (Article 23 of the Decree).

In the knowledge that understanding the single types of Offences is an essential requirement for implementing the Model, the Predicate Offences envisaged by the Decree and by the special laws supplementing it are fully referred to and described in **Annex A: Types of Predicate Offences**, of this Model.

1.1.1 Criteria for attributing liability to Entities

If one of the Predicate Offences is committed, the Entity is punishable only under given conditions, defined as criteria for attributing the Offence. These criteria are distinguished between “objective” and “subjective”.

(i) the first objective criterion to be met for the Entity to be punishable is that the Offence committed must be included in the strict and exhaustive list of **Predicate Offences** included in the Decree.

(ii) the second objective criterion is that the Offence is to be committed in the **interest** or to the **benefit** of the Entity. It therefore must have been committed in an area inherent to the Entity’s specific activities and the latter must have benefited from it, even only potentially. At least one of the two alternative conditions must be met:

- “interest” is a requirement that may be assessed *ex-ante* and it exists when the author of the crime has acted with the intent of benefiting the Entity, regardless of whether this goal has actually been achieved;
- “benefit” is a requirement that may only be assessed *ex-post* and it exists when the Entity has gained, or could have gained, from the Offence a positive result, whether financial or other.

According to the Court of Cassation (Cass. Pen. 4 March 2014, no. 10265), the notions of interest and benefit should not be regarded as a unitary notion but rather as separate, given that there is a clear distinction between what may be considered a potential gain resulting from the Offence and a benefit actually obtained as a result of the Offence. The same view has been expressed by the Court of Milan (Ord., 20 December 2004) and the Supreme Court of Cassation (see the same ruling Cass. Pen., 4 March 2014, no. 10265), according to which the fact that a criminal action aims to achieve a given benefit is in itself sufficient, regardless of whether or not it has actually been gained.

As recently reiterated by the Court of Cassation (Cass. Pen., 3 March 2021, no. 22256), interest and benefit are alternative conditions, not necessarily cumulative. As regards ascertaining the existence of the benefit requirement, even a single violation may be relevant, given that it is not instead necessary to also establish systematic violations.

The Entity’s liability is not only entailed when an immediate financial benefit has been gained from the commission of the Offence, but also if, although no benefit was gained, it was motivated by the Entity’s interest. An improvement in its position on the market or the concealment of a financial crisis situation, for instance, are cases that affect the Entity’s interests even if they do not provide an immediate and direct financial benefit.

Equally, for the purpose of establishing the Entity’s liability, proving that it has objectively obtained a benefit from the Offence is sufficient, even when it is not possible to determine the actual interest indicated prior to the commission of the Offence and as long as, at the same time, it has not been established that the latter was committed solely in the interest of the natural person or third parties who committed it (Cass. Pen., 19 January 2021, no. 15543).

(iii) the third objective criterion is that the Predicate Offence must have been committed by one or more qualified subjects, i.e. by “*persons holding representation, administration or management functions in the Entity or in one of its organizational units endowed with financial and functional autonomy*” or by persons who “*perform, also de facto, the management and control*” of the Entity (subjects in so-called “*top positions*”), or by “*persons subject to the management and supervision of one of the persons in top positions*” (so-called “*subordinates*”).

The perpetrators of the Predicate Offence which may give rise to the Entity’s administrative liability, may therefore be: (a) individuals in “*top positions*”, such as, for example, its legal representative, CEO, general director or a facility manager, as well as individuals who perform, even de facto, management and control for the Entity and (b) “*subordinate*” subjects, typically employed workers, but also subjects external to the Entity, entrusted with an assignment to be carried out under the management and supervision of the top positions.

As better specified below (see par. **Errore. L'origine riferimento non è stata trovata.**), although the adoption of the model may be a reason for non-punishability, whether the Predicate Offence has been committed by an individual in a top position or an individual in a subordinate position, the Decree is much firmer and stricter when the Offence has been committed by an individual in a top position given that, in this case, a reversal of the burden of proof applies and it is the Entity that is required to prove that the Offence

has been committed by its official in a top position fraudulently eluding the model. The Decree requires stronger evidence of non-involvement given that the Entity is required to prove a sort of “internal fraud” by individual in top positions.

In case of Offences committed by persons in subordinate position, the Entity may instead be held liable only if it is ascertained that the commission of the Offence was made possible by failure to fulfil the required management or supervision obligations. In this case, there is a real organizational weakness: the company has indirectly consented the commission of the Offence by failing to monitor activities and subjects at risk of committing a Predicate Offence.

Should more than one individual take part in committing the Predicate Offence (alleged collusion of persons in the Offence pursuant to Article 110 Italian criminal code), it is not necessary for a “qualified” subject to carry out the typical action envisaged by criminal law. It is sufficient for them to provide a consciously causal contribution to the commission of the Offence.

The subjective criterion for attributing liability is met when the Offence expresses a connotative orientation of the corporate policy or at least depends on a weakness in the organization.

The Decree’s provisions exclude the Entity’s liability if – prior to commission of the Predicate Offence – the Entity had adopted and effectively implemented an “organization and management” model suitable to prevent the commission of Offences of the kind committed (*infra*, par. **Errore. L'origine riferimento non è stata trovata.**). The Entity’s liability, from this standpoint, is linked to its “failure to adopt or comply with the due standards” relevant to the Entity’s organization and activities, a shortcoming referable to the corporate policy or to a structural and prescriptive weakness in the corporate organization.

Lastly, the Decree states the principle of autonomy of the Entity’s liability in respect of individual criminal liability: indeed, the Entity is liable also if the natural person who has committed the Offence has not been identified or is not accountable.

1.1.2 Sanctions applicable to the Entity

The Decree provides for four types of sanctions that may be imposed on an Entity because of the commission or attempted commission of Predicate Offences:

a) *Monetary sanction*

This is always applied if a judge considers the Entity liable. It is established through a system based on “quotas” (not less than one hundred and not more than one thousand), each for a value ranging between a minimum of Euro 258.23 and a maximum of Euro 1,549.37. The monetary sanctions, therefore, go from a minimum of Euro 25,823 to a maximum of Euro 1,549,370 (with the exception of corporate Offences for which monetary sanctions are doubled according to the provisions laid down by the Law on Savings, 262/2005, Article 39, comma 5). The judge will determine the number of quotas taking into account the seriousness of the Offence, the degree of responsibility of the Entity and any activities the Entity has carried out to eliminate or mitigate the consequences of the Offence and to prevent the commission of others. The quota amount is set based on the Entity’s economic and financial circumstances, for the purpose of ensuring the effectiveness of the sanction.

The monetary sanction is reduced by one third or by half if, before the first instance proceedings are declared open:

- the Entity has fully paid compensation for the damage and has eliminated the harmful or dangerous consequences of the Offence, or has in any event strived to do so;

- has adopted or brought into operation an appropriate organizational model to prevent Offences of the kind committed.

Furthermore, the monetary sanction will be reduced by half if:

- the perpetrator has committed the Offence in his/her prevalent interest or that of third parties and the Entity did not gain a benefit from it or only a minor one;
- the financial loss is especially small.

The fundamental principle guiding the entire matter of the Entity's liability, envisages that the obligation to pay the monetary sanction imposed on the Entity should fall on the Entity alone, with its assets or mutual fund. The provision, therefore, excludes any direct financial liability for Partners or associates, regardless of the legal nature of the collective Entity.

b) Disqualifying sanction

This entails disqualification from performing activities, suspension or revocation of authorizations, licences, or concessions functional to the commission of the Offence, prohibition on contracting with the Public Administration, exclusion from facilitations, funding, contributions and subsidies and possible withdrawal of any already granted and prohibition on advertising goods or services.

The duration of disqualifying sanctions should not be less than three months and more than two years.

Disqualifying sanctions are imposed, together with monetary sanctions, only if expressly envisaged for that type of Offence, and only when one of the following conditions occur:

- the Entity has already previously committed a criminal Offence (reiteration of Offences);
- the Entity has gained a significant profit from the Offence and the Offence was committed by individuals in top positions or by individuals subject to the management of others when, in this case, the commission of the Offence has been determined or facilitated by serious organizational shortcomings.

c) Confiscation

This entails acquisition by the State of the price of or profit from the Offence, also in equivalent form (confiscating, that is, a sum of money, goods or other benefits for an amount equal to the price of or profit from the Offence).

Confiscation from the Entity is always provided for with a guilty verdict, except for the portion that may be returned to the damaged party.

d) Publication of the verdict

This entails publication of the guilty verdict (in full or an extract and at the expense of the Entity) in one or more newspapers indicated by the judge and by billposting in the municipality in which the Entity has its headquarters. The judge may order publication of the verdict when a disqualifying sanction has been imposed on the Entity.

Lastly, the Prosecutor may ask for disqualifying sanctions to be applied also as a precautionary measure when there is strong evidence of the Entity's responsibility or there are well-founded and specific elements suggesting a real risk of further Offences of the kind already committed.

1.1.3 Exemption of liability: the organization, management and control model pursuant to Decree

In introducing the above regime of administrative liability, the Decree envisages a specific form of exemption from the same should the Entity prove it has adopted all the necessary organizational measures to prevent the commission of Predicate Offences by subjects operating on its behalf.

In particular, the Entity is exempt from liability if it proves:

- a) that its governing body has adopted and effectively implemented, prior to the commission of the Offence, organization, management and control model suited to preventing Offences of the kind committed;
- b) that the task of overseeing the operation and observance of the model and of updating it has been entrusted to a body of the Entity endowed with autonomous powers of initiative and control;
- c) that supervision by the above mentioned body was neither omitted nor insufficient.

The above-listed conditions must concur jointly in order for the Entity's liability to be excluded. The exemption from liability of the company therefore depends on the adoption and effective implementation of a model for the prevention of Offences and the establishment of a Supervisory Body to supervise the model, entrusted with the responsibility of monitoring the conformity of activities with the standards and procedures defined in the model.

However, adoption of the model is not itself enough to exclude the Entity's liability: it is also necessary for the model to be effective, specific and up to date.

(i) Effectiveness

The effectiveness of an organization model depends on its suitability to prevent at a practical level, or at least significantly reduce, the risk of Predicate Offences being committed. Such suitability is ensured by the existence of appropriate decision-making and preventive and subsequent control mechanisms for identifying any operations presenting anomalous features, for reporting any conduct falling within risk areas and consequently instruments for prompt intervention. The effectiveness of an organizational model, indeed, is also a function of the efficiency of suitable instruments for identifying "Offence symptomatology".

(ii) Specificity

Specificity is one of the elements characterising the effectiveness of the Model, according to Article 6, paragraph 2 letters a and b.

The specificity of the model is linked to the risk areas – and requires a census of the activities in relation to which Offences may be committed - and to the processes for the development and implementation of the Entity's decisions in "sensitive" sectors.

Similarly, the model should also identify appropriate procedures for managing financial resources and fulfilling information obligations as well as an adequate disciplinary system, while taking into account the characteristics and size of the company, the kind of activities it performs and the company history.

(iii) Up to date

As to this aspect, it should be noted that a model is suited to reducing the risk of Offences when it is constantly adjusted to the characteristics of the company structure and activities.

According to the provisions set out in Article 7 of the Decree, the effective implementation of the Model requires periodic verification and possibly changes to the same if any possible violations are discovered or changes are made to the activities or the organizational structure of the company/Entity.

Article 6 of the Decree assigns the task of updating the Model to the Supervisory Body, it being endowed with autonomous powers of initiative and control.

Adoption of a model pursuant to the Decree is not imposed by the Decree itself but, in view of the criteria for attributing the Offence to the Entity, the model is the only instrument that can, if effectively implemented, possibly avoid the involvement of the Entity in the commission of Predicate Offences. Consequently, therefore, adoption of an effective and efficient model is in the interest of the company itself.

Article 6 of the Decree, lastly, under paragraph two describes the content of the model, that should:

- a) identify the Entity's activities in connection with which Predicate Offences could possibly be committed;
- b) envisage specific protocols aimed at planning the development and implementation of the Entity's decisions in consideration of the Predicate Offences to be prevented;
- c) identify procedures for managing financial resources suited to prevent the commission of such Offences;
- d) envisage information obligations in respect of the Supervisory Body;
- e) introduce an appropriate internal disciplinary system to sanction failure to comply with the measures indicated in the model;
- f) envisage one or more channels that will enable "top positions" or "subordinates" to present, in order to protect the Entity's integrity, detailed reports on any relevant unlawful conduct in respect of the Decree and based on accurate and concurring factual elements, or of violations of the model of which they have become aware in connection with the functions they perform.

1.1.4 Offences committed abroad

The liability envisaged by the Decree also applies in relation to Offences committed abroad by the Entity, on condition that:

- a. the Offence has been committed by a subject functionally tied to the Entity, whether in a top or subordinate position, as indicated above;
- b. the Entity has its headquarters in Italy;
- c. there are the overall conditions for action to be undertaken as envisaged by articles 7, 8, 9 and 10 of the Italian Criminal Code to prosecute in Italy an Offence committed abroad (should the law envisage that the natural person be punished at the request of the Ministry of Justice, action may be taken against the Entity only if the request also concerns the Entity itself);
- d. the State of the place where the Predicate Offence has been committed does not take action.

1.2 The function of the Model according to the Decree

Although it is envisaged by the law as optional and not mandatory, the adoption of the Model, has been regarded by F2M eSolutions as a significant opportunity to implement "active" prevention of Predicate Offences, by strengthening its Corporate Governance and Internal Control System, as well as disseminating the appropriate ethical and conduct principles.

The Model identifies - in accordance with the Code of Ethics adopted by the Company of which it is an integral part – the rules and procedures to be observed by all those to whom they are addressed, *i.e.* by those who, like Employees, Corporate Bodies, Service Companies, Consultants and Partners, operate on behalf or in the interest of the Company in the area of Sensitive Processes that could entail liability pursuant to Decree.

The Supervisory Body, appointed for the purpose, ensures ongoing oversight on the implementation of the Model, through monitoring and the possible imposition of disciplinary or contractual sanctions aimed at effectively censuring any unlawful conduct.

1.3 Reference Guidelines

In developing this Model, F2M eSolutions has taken its inspiration from the **Reference Guidelines** adopted by Confindustria, whose principles are described in **Annex B: Reference Guidelines** and referred to in the text of this Model.

The Reference Guidelines, adopted in March 2002, were lastly updated in June 2021.

It remains understood that given that the Model needs to be drawn up taking into consideration the actual reality of the Company, it might differ from the Reference Guidelines that, by their very nature, are generic.

SECTION II – THE COMPANY

2.1 Free2Move eSolutions S.p.A.

Free2Move eSolutions S.p.A. (“**F2M eSolutions**” or the “**Company**”) is a joint stock company, whose shares are held for 49% by NHOA Energy S.r.l. (previously ENGIE EPS Italia S.r.l.) and for 51% by FCA Italia S.p.A., active in the design, realization and supply of *e-mobility* products and services. In particular, the Company develops innovative technologies to drive the transition to electric mobility and offers recharging solutions and services to make the transition intuitive and seamless.

In more detail, the Company’s purpose is research, conception, creation, realization, construction, development, production, marketing, installation, maintenance, assistance and modification of products, systems, infrastructures, services (also in the shape of subscriptions) and accessory systems for the use, accumulation, transportation and distribution of electricity as well as providing power and recharging of batteries and electric vehicles, also in cooperation with public and private research institutes, private enterprises, universities, foundations, local, national and international institutions and, more generally, with any public or private party interested in the development of new technologies and applications in the energy, environmental and electric mobility sectors.

2.2 The Ethics & Compliance of F2M eSolutions

F2M eSolutions has adopted Ethics&Compliance regulations made up of:

- A Code of Ethics that constitutes the foundations on which all reference documents, policies and codes of conduct adopted by the Company are based;
- The policies and procedures adopted by the Company;
- the Codes of conduct.

2.3 The current organization of the Company

The Company has organised its business and internal activities according to the structures presented in detail in the corporate organizational chart (see **Annex D**).

Basically, F2M eSolutions carries out its activities at its headquarters in Milan, in Piazzale Lodi 3 and at local units in Milan and Turin.

F2M eSolutions also carries out its activities at clients’ facilities. These activities are defined as the occasion rises with the customer on the basis of an approved agreement.

2.4 The Corporate Governance system

The structure of the F2M eSolutions corporate and control bodies is as follows:

- a. the shareholders NHOA Energy S.r.l. and FCA Italy S.p.A.;
- b. the Board of Directors with a Chairman, a Managing Director and a General Director.

Further details concerning the composition of the Board of Directors are available in the Company registration document (see **Annex E**).

SECTION III – CONSTRUCTION OF THE MODEL

3.1 The F2M eSolutions

1.1.1 The Model's inspiring principles and elements

The development of the Model, in addition to the provisions set out by the Decree, also took into account the procedures and control systems, identified in the “*as-is*” stage as already operational in the Company and considered suitable also as measures for preventing Offences and for control over Sensitive Processes. In particular, the following were found to be already operational in F2M eSolutions:

- The Code of Ethics, that expresses the principles of the “corporate deontology” recognised as its own and which the Company requires all Employees, Corporate Bodies, Consultants and Partners to observe;
- the principles of Corporate Governance that reflect applicable law and international best practices;
- the Internal Control System (and hence, corporate procedures, documentation and indications concerning the hierarchical, functional and organizational structure and the management control system);
- regulations concerning the administrative, accounting, financial and reporting systems;
- internal communications and staff training;
- the disciplinary system described in the CCNL Metalworkers and the CCNL Journalists;
- more generally, applicable Italian and foreign legislations (including, for example, the laws on safety at the workplace).

1.1.2 The Model's features

In line with the Decree's provisions, the Model complies with the legal requirements of effectiveness and specificity and of being up to date. In particular, the Model envisages decision-making and *ex-ante* and *ex-post* control systems suited to identify “anomalous” operations and alert to any conduct falling within a risk area, in addition to providing the means for prompt intervention. The Model has also been drawn up on the basis of specific risk areas that emerged from a census of activities pertaining to the Company (see, more specifically, next paragraph below), and of the current structure of the Company itself, in the awareness of the need to proceed with updating and/or amending it if significant breaches of its provisions are identified, or if changes are made to the Company's organization or activities.

1.1.3 Method used to construct the Model

The Company carried out a careful analysis of its organization, management and control instruments (in particular, through an analysis of the Company's history, the corporate context, the sector in which it operates, its organizational structure, the existing governance system, the system of delegations and proxies, its main existing legal relationships with third parties, its operational environment, the practices and procedures formalised and disseminated inside the Company. The purpose of the analysis was to verify the correspondence of already adopted behavioural principles and procedures with the aims envisaged by the Decree and, should it be considered necessary, to initiate an adjustment process. Indeed, in Article 6, paragraph 2, letter a), the Decree expressly envisages that the Entity's Model should identify corporate activities in relation to which Predicate Offences could potentially be committed.

The drafting of the Model was preceded by a series of preliminary activities divided into different stages and all aimed at the construction of a system for risk prevention and management in line with the Decree's provisions and also, in addition to them, inspired by the Reference Guidelines and the best practices

provided for by the most advanced national and international legislative instruments in the fight against corporate criminality.

a) **Identification of Sensitive Processes (“as-is analysis”)**

In order to identify the sectors in which there is a greater likelihood of the risk of Offences being committed and the way in which they may be committed, an analysis was made of the corporate documentation (organizational charts, activities carried out, main processes, minutes of Board meetings, proxies, organizational instructions, risk assessment document, etc.) and key persons within the corporate structure were interviewed (for instance, CFO, head of legal Affairs, head of Human Resources, Head of Security etc.).

An analysis was therefore made of F2M eSolutions’ corporate activities and related organizational structures in order to identify the areas of activity in relation to which Predicate Offences may be committed, examples of possible ways of committing them and the processes which might give rise in their performance to the conditions and provide the means for committing such Offences (instrumental/functional processes).

The areas of At-Risk Activity of Predicate Offences being committed and of Sensitive Processes were analysed also through interviews with the corporate persons of reference for each management area (with questions targeted to an in-depth analysis of Sensitive Processes and control over the same – existing procedures, the possibility of documenting operations and controls, separation of functions, etc.), and as such equipped with the broadest and deepest knowledge of operations in each sector of the corporate activities.

b) **Mapping of Offence risks**

For each Offence-risk, sensitive activities/processes instrumental to such Offence-risks were identified, as well as the corporate structures responsible for operational activities in such areas and that oversee such activities. An assessment of the risk level to which the Company is exposed was made when the corporate activities were mapped in relation to each sensitive activity and each instrumental/functional process, on the basis of quantitative and qualitative considerations that took into account some factors such as the frequency of occurrence of the event or activity, the seriousness of the sanctions potentially associated with commission of one of the Offences and the damage resulting from possible unlawful conduct in the At-Risk Activity.

The results of the above-described mapping activity were collected in a descriptive chart that provides details of the distinct profiles for the risk of committing the Offences considered by the Decree, in connection with the Company’s activities. The self-risk assessment document is kept at the Company headquarters.

c) **Gap analysis**

Based on existing controls and procedures relating to Sensitive Processes and to the provisions and aims of the Decree, it was possible to identify actions to improve the current Internal Control System (processes and procedure) and some essential organizational requirements for the definition of a “specific” organization, management and monitoring Model in accordance with the Decree.

1.1.4 The Model’s structure

The Model is organised in sections containing principles and general rules of conduct, drawn up to prevent the commission of Predicate Offences (reported in **Errore. L'origine riferimento non è stata trovata.: Types of Predicate Offences**). In particular, Section VI, under par. 6.2.1 F2M eSolutions’ Sensitive Processes, (i) identifies the Sensitive Processes and Instrumental Activities posing an Offence risk within

the corporate activities, connecting them to the single types of Predicate Offences, (ii) identifies general and/or specific principles of conduct.

1.1.5 The Model's Recipients

The provisions laid down in the Model are binding for:

- a) administrators and all those who perform, also de facto, management, administration, direction and control functions, as well as functions of a disciplinary, advisory and consultative nature in the Company or in one of the autonomous units in its organization;
- b) Company Employees, *i.e.* all those who are tied to the Company by a subordinate work relationship, even if seconded abroad to perform their activities;
- c) all the individuals who cooperate with the Company on the basis of a para-subordinate work relationship and individuals subject to the direction or supervision of the Company's management;
- d) distributors, commercial Partners and agents that operate on behalf of the Company;
- e) individuals who, while not belonging to Company, operate on the basis of an assignment or on its behalf as attorneys, Consultants, etc.;
- f) parties that act in the interest of the Company based on their connection with it established by legal contractual relationships or other kinds of agreements such as, for example, Partners or third parties involved in the realization or acquisition of a project.

The Supervisory Body, having been consulted by the head of the area/function involved, shall resolve any doubts concerning applicability or the procedures for applying the Model to a subject or a category of third parties.

1.1.6 Adoption of the F2M eSolutions Model and subsequent amendments

The Model was adopted with a resolution of the Board of Directors of F2M eSolutions that also established the Supervisory Body.

Each member of the Board of Directors, and also of the Company's Board of Auditors, has undertaken to observe the Model.

Given that this Model is an act of enactment of the governing body (in conformity with the provisions of Article 6, paragraph I, letter a) of the Decree) any amendments and additions fall under the responsibility of the Board of Directors.

The Board of Directors may delegate specific amendments to the Managing Director, notwithstanding that it will be required to ratify any changes made on a yearly basis.

1.1.7 Implementation of the F2M eSolutions Model

The responsibility for implementation of the Model in relation to identified Sensitive Processes lies exclusively with F2M eSolutions, that has attributed to its Supervisory Body the task of performing the relevant controls according to the procedures described in the Model itself.

In order to concretely implement Model and ensure that it is aligned to the current organizational and operational reference context, and applicable Offence risk control and prevention systems are always kept up to day, each corporate person of reference has a duty to define and keep up to date the organizational documents that regulate the processes in their area of responsibility, in agreement with the structure competent for organization and processes, that will be required to ensure an assessment of the

organizational consequences, the orientation of consequent actions, the adoption of a shared language and methodological approach, consistency with the organizational structure, with the documentation concerning laws currently in force or about to be issued and with the system of delegations and proxies in force.

Corporate persons of reference are also required to draw up and ensure regular information flows to the Supervisory Body, through which they may report any possible issues found in the implementation of the Model and possible areas of improvement.

3.2 The Supervisory Body

3.2.1 Identification of the Supervisory Body: appointments and dismissals

The Decree envisages that the body to be entrusted with the task of overseeing operation and observance of the Model, and handling its updates, should be a Company body endowed with autonomous initiative and control powers (Article 6. 1, *b*) of the Decree).

The Reference Guidelines suggest that this should be a body in the Entity other than the Board of Directors, characterised by autonomy, independence, professionalism and ongoing action, as well as honourability and the absence of conflicts of interest.

In implementation of the provisions laid down by the Decree, F2M eSolutions has established, with a Board of Directors' resolution, a Supervisory Body made up of three full members.

The above members have been recognised as being the best suited to take on this role, given the following requirements that each of them meets, in line with the Decree's provisions, the Reference Guidelines and case law:

- **autonomy and independence.** The Supervisory Body should be free of any influence resulting from ties of subordination to the control unit and should be a third body in a position also of hierarchical independence, capable of adopting autonomous measures and initiatives. It is also essential for the Supervisory Body not to perform any operational duties, *i.e.* not to be directly involved in the management activities that are the object of its supervisory activities. The Supervisory Body must enjoy autonomy in decision making, be described as the essential freedom of self-determination and action, with the full right to technical discretion in performing its functions;
- **honourability.** A person may not be appointed member of the Supervisory Body and, if necessary, will be dismissed, if he/she has been disqualified, incapacitated or bankrupt or in any event convicted for one of the Offences envisaged by the Decree or, moreover, given a sentence entailing disqualification, even temporary, from public office or the ability to hold management positions;
- **proven professionalism.** The Supervisory Body must have specific capabilities in terms of inspection and advisory activities, as well as technical and professional skills suited to the performance of analyses of control systems and pertaining to legal and criminal matters. As regards matters concerning health and safety at the workplace, the Supervisory Body should avail itself of the resources activated for the management of the relevant aspects (RSPP – Head of the Prevention and Protection Service, ASPP – Prevention and Protection Service Operators, RLS – Workers' Safety Representative, MC – Competent Physician, first aid operators, fire emergency operator). Such persons and the Supervisory Body perform their duties at different levels, within an integrated internal control system. In particular, the Head of the Prevention and Protection Service performs technical-operational checks (1st level control), while the Supervisory Body checks on the efficiency and effectiveness of the procedures relevant to the Decree (2nd level control).

Normally, in the performance of its supervisory and control duties the Company's Supervisory Body is supported by the Internal Audit function.

- **ongoing action.** The Supervisory Body should perform the activities required for supervision of the Model on an ongoing basis with appropriate diligence and the necessary investigative powers;
- **availability of the organizational and financial means** needed to perform its functions. The independence of the Supervisory Body is, furthermore, ensured by the governing body's obligation to approve, when drawing up the corporate budget, the adequate allocation of financial resources, as proposed by the Supervisory Body itself, which the latter may use for any needs arising in connection with the proper performance of its duties (e.g. specialised consultancies, travel, etc.).

The Supervisory Body of F2M eSolutions is a collegial body made up of three members chosen from amongst individuals with specific professional skills and experience in corporate matters and inspection activities. In particular, individuals from either inside or outside the Entity may be called upon to become members of the Supervisory Body, on condition that they meet the above requirements of autonomy and independence. In case of a mixed composition, given that the individuals who work within the Company cannot be required to have full independence from the Entity, the degree of independence of the body should be assessed as a whole. The above persons exercise their decision-making powers separately and will they themselves provide for a mechanism aimed at avoiding the adoption of conflicting decisions that will require action to resolve any issue on the part of the Managing Director.

The responsibility for defining the aspects pertaining to continuity in the actions of the Supervisory Body, such as the scheduling of activities, taking minutes of its meetings and regulating information flows from the corporate structures, lies with the Supervisory Body, that may define its internal mode of operation by specifically regulating its activities (establishing the frequency of controls, identifying analysis criteria and procedures, etc.).

The members of the Supervisory Body will have a 3 (three)-year mandate, renewable following a resolution in this regard by the Board of Directors, that also has the power to dismiss, for just cause, all or some of the members of the Body itself, no later than 60 (sixty) days prior to each deadline.

In case of withdrawal, incapacitation, death or forfeiture of a member of the Supervisory Board, the latter will promptly notify the Board of Directors that will without delay replace him/her.

The following are causes of ineligibility or forfeiture for members of the Supervisory Body:

- a) the condition of having been subjected to prevention measures applied by the judicial authority pursuant to Law no. 1423 dated 27 December 1956 (law on prevention measures applied to people who are a threat to safety and public morality) or Law no. 575 dated 31 May 1965 (provisions against organised crime);
- b) the condition of having been convicted, even if the sentence is not yet final or has been issued pursuant to articles 444 et seq. Code of Criminal Law (plea bargain) or even if the sentence is conditionally suspended, notwithstanding the effects of the rehabilitation (i) for one or more Offences among those envisaged by the Decree, or (ii) detained for a period of no less than two years for any Offence committed with intent;
- c) the condition being disqualified, incapacitated, bankrupt or having been convicted, even with a non-final judgment, with a sentence entailing disqualification, even temporary, from public office or the incapacity to perform management offices.

The presence of even one of the above conditions entails ineligibility to the position of member of the Supervisory Board and, in case of election, automatic forfeiture of said position, without the need for a resolution of dismissal by the Board of Directors that will provide for a replacement.

The following are the conditions that legitimise dismissal for just cause:

- a) the loss of eligibility requirements;
- b) failure to fulfil the obligations inherent to the entrusted mandate;
- c) the absence of good faith and diligence in performing the mandate;
- d) non-cooperation with the other members of the Supervisory Board;
- e) unjustified absence at one or more Supervisory Board meetings.

In the presence of just cause, the Board of Directors will revoke the appointment of the no longer eligible member of the Supervisory Board and, having provided adequate motivation, will provide for his/her immediate replacement.

Every member of the Supervisory Board may withdraw at any time from the position, with minimum notice of one month with a written and communication and justification to the Board of Directors.

In case of forfeiture or withdrawal by one of the members of the Supervisory Board, the Board of Directors will promptly provide for the replacement of the member who has become ineligible, notifying also the Chairman of the Supervisory Board.

3.2.2 Functions and powers of the Supervisory Body

The Supervisory Body is entrusted with the task of overseeing:

- compliance with the Model by Employees, Corporate Bodies, Service Companies, Consultants and Partners;
- the effectiveness and adequacy of the Model in relation to the corporate structure and its actual ability to prevent the commission of Offences;
- the appropriateness of updating the Model, should this become necessary in relation to changed corporate and/or regulatory conditions.

To this end, the Supervisory Body is guaranteed free access – at all the Company's functions, without the need for prior consent – to any corporate information, data or document considered relevant to the performance of its duties and should be constantly informed by the management on: a) the aspects of corporate activities that may expose F2M eSolutions to the risk of one of the Offences being committed; b) relations with the Service Companies, Consultants and Partners that operate on behalf of the Company in the area of Sensitive Operations; c) extraordinary Company operations.

In particular, the Supervisory Body:

- performs surveys of Company activities in order to update the mapping of Sensitive Processes;
- verifies compliance with the methods and procedures foreseen by the Model and detects any behavioural deviations that may emerge from the analysis of the information flows and from the reports to which the heads of the various functions are subject;
- gathers, processes and stores information relevant to compliance with the Model, and updates the list of information that must be transmitted to it or kept at its disposal;

- coordinates with the Company departments (also through specific meetings) for the best monitoring of the activities in relation to the procedures established in the Model and to assess the adequacy and updating needs of the Model;
- interprets the relevant regulations (in coordination with the function in charge of Legal Affairs) and verifies the adequacy of the Model to these regulatory prescriptions;
- makes proposals to the Board of Directors for any changes and/or additions that may become necessary as a result of significant violations of the Model's prescriptions, significant changes to the Company's internal structure and/or to the way in which business activities are carried out, as well as regulatory changes;
- periodically carries out targeted checks on certain operations or specific acts carried out by the Company, especially within the scope of the Sensitive Processes, the results of which must be summarized in a special report to be submitted to the designated Corporate Bodies;
- reports to the Board of Directors any ascertained violations of the Organizational Model that may entail the occurrence of a liability on the part of the Entity and coordinates with the Company's management in order to evaluate the adoption of any disciplinary sanctions, without prejudice to the latter's competence for the imposition of the sanction and the related disciplinary procedure;
- coordinates with the manager of the department in charge of managing Human Resources in defining training programs for Employees and the content of periodic communications to be given to Employees and Corporate Bodies, also through the Company's Intranet, aimed at making them aware of, and providing them with basic knowledge of, the regulations set forth in the Decree;
- activates and conducts internal investigations, liaising from time to time with the Company departments concerned, in order to acquire further elements of investigation (e.g. with the department in charge of Legal Affairs for the examination of contracts that deviate in their form and content compared to standard clauses aimed at guaranteeing the Company from the risk of involvement in the commission of Offences; with the department in charge of Human Resources for the application of disciplinary sanctions, etc.);
- periodically verifies, with the support of the other competent functions, the system of proxies and powers of attorney in force and their consistency with the entire system of organizational communications (such as internal Company documents by which the proxies are conferred) recommending possible changes in the event that the management power and/or qualification do not correspond to the powers of representation conferred on the proxy holder or there are other anomalies;
- indicates to the management any required changes to the systems for managing financial resources (both incoming and outgoing), already present in the Company, in order to introduce some suitable means to detect the existence of any financial flows characterized by more discretion than what is normally foreseen.

The activities performed by the Supervisory Body cannot be criticised by any other corporate organism or body, notwithstanding that the managing body is entrusted with the task of verifying the adequacy of its interventions, since the managing body has the ultimate liability for the functioning of the Model.

3.2.3 Reporting by the Supervisory Board to top management

The Supervisory Board reports on the implementation of the Model and the emergence of any critical issues.

The Supervisory Body has two lines of reporting:

- the first, on an ongoing basis, directly to the Managing Director;

- the second, to the Board of Directors and the Board of Auditors, reporting at least annually on the activities carried out (controls and their outcome, the specific checks referred to in point 3 below and their outcome, any updates to the mapping of Sensitive Processes, etc.).

In the event the Supervisory Board detects critical issues that can be referred to any of the members of the Board of Directors or the Board of Auditors, the corresponding report must be addressed promptly to one of the other subjects not involved.

Meetings with the bodies to which the Supervisory Board reports must be recorded in minutes, and copies of the minutes must be kept by the Supervisory Board and the bodies involved from time to time.

The Board of Statutory Auditors, the Board of Directors and the Managing Director have the power to convene the Supervisory Board at any time, which, in turn, has the power to request, through the competent functions or subjects, convening of the aforesaid bodies for urgent reasons.

3.2.4 Information flows to the Supervisory Body

Within the scope of its powers of action and control, the Supervisory Body receives from the appropriate Company functions the information required to perform its task of supervising the functioning of and compliance with the Model as well as its updating. In particular, the following information concerning the management of Sensitive Processes must be mandatorily sent to the Supervisory Body:

- findings and sanctions levied by Public Bodies (Agenzia delle Entrate, Ispettorato del Lavoro, INPS, INAIL, ARPA, ASL, etc.) as a result of inspections;
- measures and/or news coming from judicial police bodies, or from any other authority, from which it can be inferred that investigations are being conducted, even against unknown persons, for the Predicate Offences that may involve the Company;
- decisions relating to the request for, disbursement and use of public financing, grants, contributions, subsidies;
- requests for legal assistance forwarded by Managers and/or Employees who are being prosecuted by the Judiciary for Offences envisaged by the regulations;
- information relating to disciplinary proceedings out and any sanctions imposed in accordance with the Model (including measures against Employees) or measures to dismiss such proceedings with the related reasons;
- organizational changes;
- any transactions relating to share capital;
- any successful cases of computer fraud concerning payments made to suppliers' bank accounts;
- requests to open/close bank accounts to be managed/operated independently by the Company;
- changes in the proxies entitled to use bank accounts to be managed/operated independently by the Company.

Third parties with whom the Company has business dealings are periodically monitored in order to exclude their inclusion in black-lists of persons at risk of terrorism (UN, EU and OFAC lists).

With specific reference to the information that must be provided to the Supervisory Body regarding environmental, health and safety issues, reference is made to Annex C.

The Supervisory Body shall be informed of the results stemming from the periodic filling in of dedicated self-assessment questionnaires by the Company management and of any improvement actions that may be established. The outcome of this analysis provides an updated picture of the Sensitive Processes and Risk Activities of the Company, in accordance with Article 6 of the Decree, and constitutes an information flow to the Supervisory Body in relation to monitoring activities to be included in the annual Supervisory Program.

Therefore, the Company's managers, directors, Employees, and collaborators shall collaborate as much as possible with the Supervisory Body by sending by e-mail any information that may be useful for the performance of its functions, to the address: odv@f2m-esolutions.com.

3.2.5 Information collection and storage

Any information, notifications and reports provided for in this Model are stored by the Supervisory Body in a special database (computerized or hard copy), in compliance with confidentiality and privacy regulations.

3.3 Whistleblowing system

Employees, Corporate Bodies, Service Companies, Consultants and Partners are required to report violations entailing an unlawful conduct, pursuant to the Decree or the Model, of which they have become aware.

Anyone wishing to make a report may contact one of the channels indicated in the Code of Ethics, available on the Group's intranet and website.

Whistleblowers reporting in good faith shall be protected against any form of retaliation, discrimination or penalization and in any case the identity of the whistleblower shall be kept confidential, without prejudice to legal obligations and protection of the rights of the Company or persons accused in bad faith.

In compliance with with the provisions of the Code of Ethics, no one may be dismissed, fired, suspended, threatened, harassed or intimidated as a result of a report made in good faith.

Anyone who retaliates against a person who has reported in good faith, or who makes an intentionally false and unfounded report, will be subject to disciplinary proceedings that may even result in dismissal, in compliance with the provisions of the Code of Ethics and Section IV of this Model.

The Supervisory Body will be kept informed of any significant reports.

3.4 Checks on the adequacy of the Model

The Supervisory Body periodically verifies the real effectiveness of the Model in preventing the commission of Offences, making use, as a rule, of the Internal Audit function and of the support of other internal functions that, from time to time, become necessary for this purpose.

This activity takes the form of sample checks of the main corporate acts and of the most important contracts concluded by F2M eSolutions in relation to Sensitive Processes and to their compliance with the rules set out in the Model, as well as of the Employees' and Corporate Bodies' knowledge of the Company's quasi-criminal liability. Furthermore, a review of the reports received during the year, of the actions taken by the Supervisory Body and of the events considered risky is performed.

The checks and their outcome are reported to the Board of Directors and the Board of Auditors.

SECTION IV - CIRCULATION OF THE MODEL

Knowledge of the Model is essential to raise awareness among all Recipients who work on behalf of and/or in the interest of the Company within the scope of the Sensitive Processes, that they may incur in Offences liable to significant criminal consequences, not only for themselves but also for the Company, in the event of any conduct contrary to the provisions of the Decree and the Model.

4.1 Employee training and information

F2M eSolutions shall guarantee accurate information/training on the content of the Model, both to the resources already working in the Company and to those to be recruited, of the rules of conduct contained therein, with a different degree of detail in relation to the different level of involvement of said resources in Sensitive Processes.

The information and training system is supervised and supplemented by the Supervisory Board's activities in this field, in collaboration with the head of the function responsible for Human Resources and with the heads of the other functions involved from time to time in the application of the Model.

Initial communication

Once the Model has been approved and/or modified by the Board of Directors, it is published on the Group's website www.esolutions.free2move.com and sent via the Company intranet to all Employees, who are required to comply with it.

Newly hired Employees, on the other hand, will receive a set of information (e.g. Code of Ethics, CCNL Metalworkers/Journalists, Model, Decree, etc.), to ensure they receive the most important information. They will also be asked to sign a declaration certifying their knowledge and acceptance of the Model and compliance with the contents described therein.

The methods for distributing the Model to other subjects required to comply with its contents (suppliers, external collaborators and third parties in general) will be established from time to time.

Training

The training activity aimed at spreading knowledge of the regulations set forth in the Decree differs, in terms of content and delivery methods, depending on the Recipients' qualifications, the risk level of the area in which they operate, whether or not they hold representation functions for the Company. The training activity is periodically repeated.

In particular, the Company has foreseen different levels of information and training through suitable means of circulation.

The Supervisory Body is also responsible for checking the contents of the training programs as described above.

All training programs shall have a minimum common content consisting of an illustration of the principles of the Decree, of the elements that make up the Model, of the individual types of Offences provided for by the Decree and of the conduct considered sensitive in relation to the commission of the aforementioned Offences.

In addition to this common matrix, each training program shall be tailored in order to provide its users with the tools required for the full compliance with the Decree in relation to the scope of operations, the duties of the recipients of the program itself, the risk level of the area in which they operate and whether or not they hold representation and management positions within the Company.

The training methods adopted consist of:

- primarily, e-learning courses delivered on the Company's IT platform via the corporate intranet;
- classroom/seminar training sessions.

These activities are run in close coordination with the Supervisory Body.

Participation in the training programs described above is compulsory; signatures proving attendance/participation are collected, and control of actual attendance is entrusted to the Supervisory Body.

The training documentation is filed and made available to the Supervisory Board.

An unjustified absence from training sessions constitutes a disciplinary Offence and entails the application of the disciplinary sanctions set out in SECTION V below - SANCTIONS SYSTEM.

The learning assessment of training is performed by means of specific tests at the end of each training program. Resources that have not passed the learning tests are subject to new training cycles.

4.2 Information to Service Companies, Consultants and Partners

Appropriate information on the policies and protocols adopted by the Company on the basis of the Model will be provided to external collaborators. The contracts to be signed by F2M eSolutions with third parties will contain explicit contractual clauses concerning compliance with the obligations and principles deriving from the Model and the Code of Ethics. Moreover, at the end of the qualification process, each newly selected supplier shall commit to comply with the Code of Ethics, the Anti-Corruption Guidelines, the policy "Ethics of Business Relationship: Governing Principles" and the obligations and principles resulting from the Model.

4.3 Information to Directors and Auditors

This Model is delivered to each Director and Auditor, who undertakes to comply with it.

SECTION V - DISCIPLINARY SYSTEM

5.1 Function of the disciplinary system

F2M eSolutions condemns any behaviour that deviates not only from the law, but also from the provisions of the Model and the Code of Ethics, even if such behaviour is committed in the interest of the Company or with the intention of bringing it an advantage.

The definition of a system of sanctions (commensurate with the violation and having a deterrent effect), applicable in the case of violation of the rules set out in this Model, makes the supervisory action of the Supervisory Body efficient and it is intended to ensure the effectiveness of the Model itself. The definition of this disciplinary and/or contractual sanctioning system constitutes, in fact, pursuant to Article 6 first paragraph letter e) of the Decree, an essential requirement of the Model itself for the purposes of exempting the Company from liability. In this regard, in fact, Article 6 paragraph 2, letter e) of the Decree provides that the organization and management models shall "*introduce a disciplinary system capable of sanctioning the failure to comply with the measures indicated in the model*".

The application of the disciplinary system and of the relevant sanctions is independent of the conduct and outcome of the criminal proceedings that may be initiated by the judicial authority in the event that such conduct is also considered to be an Offence under the Decree.

This is without prejudice to any claim for compensation for any damages caused to the Company by conduct in violation of the rules set out in the Model, as in the case of a judge applying the precautionary measures set out in the Decree.

The assessment of infringements may also be initiated at the request of the Supervisory Body if, in the course of its control and supervisory activities, it has detected a possible infringement of the Model.

Sanctions against managers, Employees and executives fall within the competence of the Managing Director and the delegated authorities for this purpose in full compliance with the delegated powers.

The Supervisory Body may also be called upon to act in an advisory capacity throughout the entire disciplinary procedure in order to acquire possible information that may be useful in view of the constant updating of the Model. The ascertainment of any responsibilities deriving from the violation of the Model and the attribution of the consequent sanction must in any case be carried out in compliance with the regulations in force, the protection of privacy, dignity and reputation of the persons involved.

In general, violations may be attributed to the following behaviors and classified as follows:

- a) conducts that include the types of Offences referred to in the Decree;
- b) conducts which, although not representing a criminally relevant Offence, are unequivocally aimed at violating the Model;
- c) conducts that do not comply with the Protocols or Procedures referred to in the Model or the Code of Ethics;
- d) uncooperative behaviours towards the Supervisory Body, consisting, by way of example, but not limited to, refusal to provide the information or documentation requested, failure to comply with the general and specific instructions given by the Supervisory Body in order to obtain information considered essential for the performance of its duties, failure to participate without justification, in inspections or interviews scheduled by the Supervisory Body, failure to attend training sessions, or, more generally, violation of the obligations to provide information to the Supervisory Body;

e) violation of confidentiality requirements towards those who make reports or retaliatory or discriminatory acts against the person(s) who has (have) made reports in accordance with the provisions of this Model.

5.2 Measures against middle managers, white collar and blue collar workers

5.2.1 Disciplinary System

Any conduct in breach of this Model on the part of Employees subject to the CCNL Metalworkers and CCNL Journalists applied to the Company constitutes a disciplinary offence.

Failure by Employees to comply with the provisions and procedures laid down in the Model and the principles established in the Code of Ethics constitutes a breach of the obligations arising from the employment relationship pursuant to Article 2104 of the Italian Civil Code and a disciplinary offence.

In compliance with the procedures provided for in Article 7 of Law no. 300 of 20 May 1970 (Workers' Charter) and any applicable special regulations, the following sanctions may be imposed on Employees:

- (a) verbal or written reprimand;
- (b) fine not exceeding the amount of 4 hours of standard pay;
- (c) suspension from duty or pay for a period not exceeding 3 days if CCNL Metalworkers is applicable or not exceeding 5 days in case CCNL Journalists is applicable;
- (d) disciplinary dismissal with the right to notice and dismissal for just cause without notice.

If the above-mentioned Employees have a power of attorney including the power to represent the Company externally, the application of a sanction heavier than a fine shall be followed by the automatic cancellation of the power of attorney.

In order to highlight the correlation criteria between violations and disciplinary measures, it is specified that

a) an employee who, as a result of mere negligence, violates the internal procedures provided for or referred to in this Model and/or the provisions of the Code of Ethics, or who, in the performance of activities in areas at risk, adopts a conduct in violation of the provisions of the Model itself and of the Code of Ethics, shall be subject to a verbal or written reprimand, depending on the seriousness of the offence, since such conduct constitutes a breach of contract entailing a prejudice to the discipline and ethics of the Company without external relevance;

b) a fine not exceeding the amount of 3 hours of the standard remuneration shall be imposed on any employee who

- has, during the two-year period, repeatedly committed infringements for which a written reprimand is applicable; or
- due to the level of hierarchical or technical responsibility, or in the presence of aggravating circumstances, undermines the effectiveness of the Model with behaviours such as, by way of example but not limited to: i) failure to comply with the obligation to inform the Supervisory Body; ii) repeated failure to comply with the formalities envisaged by the procedures and prescriptions indicated in the Model, in the event that they concern a procedure or relationship in which the Public Administration is a party;

c) the disciplinary measure of suspension from service and from pay for a maximum of 3 days (CCNL Metalworkers) or 5 days (CCNL Journalists) shall apply to any employee who

- commits multiple violations (at least 3 times), during the two-year period, of those referred to in letter a) above, or for which a fine not exceeding the amount of 3 hours of the standard remuneration is applicable;
- in violating the internal procedures foreseen by the Model or by the Code of Ethics, causes damage to the Company or exposes it to an objective danger for the integrity of the Company's assets, such as, purely by way of example, violation of the conduct to be adopted in the management of donations or gratuities, or of the provisions concerning signature powers and the system of delegated powers attributed with regard to acts and documents addressed to the Public Administration;

d) is subject to disciplinary dismissal:

- with right to notice, an employee who engages in repeated failures entailing the suspension referred to in letter c) above;
- for just cause without notice, an employee who (i) fraudulently circumvents the procedures and prescriptions of the Model and/or of the Code of Ethics by means of conduct unequivocally aimed at committing one of the Predicate Offences or (ii) violates the internal control system by removing, destroying or distorting documentation or by preventing control of or access to information and documentation by the parties in charge, including the Supervisory Body, in such a way as to prevent the transparency and verifiability thereof.

The Company shall not adopt any disciplinary measure against an employee without complying with the procedures laid down in the CCNL Metalworkers/Journalists for individual cases.

The type and extent of the above-mentioned sanctions imposed on Employees must, when applied, be commensurate with the principle of proportionality provided for in Article 2106 of the Italian Civil Code, taking into account for each case:

- a) the intentionality and the degree of repetition of the conduct, the degree of negligence, imprudence or inexperience with regard also to the foreseeability of the event;
- b) the objective seriousness of the fact that represents a disciplinary infringement;
- c) the overall conduct of the employee with particular regard to the existence or otherwise of previous disciplinary records , within the limits permitted by law;
- d) the employee's duties;
- e) the functional position of the persons involved in the facts constituting the failure; and
- f) other particular circumstances accompanying the disciplinary violation.

With regard to the ascertainment of infringements, disciplinary proceedings and the imposition of sanctions, the powers already conferred, within the limits of their respective competences, on Company management remain unchanged.

5.2.2 Model Violations and Sanctions

The following behaviours are punishable as violations of this Model

- violations, by an employee, of internal procedures provided for by this Model or the adoption, in the performance of activities related to the Sensitive Processes, of behaviors that do not comply with

the prescriptions of the Model whether or not they expose the Company to an objective situation of risk of committing one of the Predicate Offences;

- any conduct that does not comply with the prescriptions of this Model and that is unequivocally directed towards the commission of one or more Offences;
- conduct in violation of the provisions of this Model, leading to the actual and/or potential application against the Company of the sanctions set out in the Decree.

The sanctions, both of a disciplinary and contractual nature, and any request for compensation for damages, shall be commensurate with the level of responsibility and autonomy of the Employee, or the role and strength of the relationship of trust connected with the assignment given to the Directors, Auditors, Service Companies, Consultants and Partners.

The system of sanctions is subject to on-going verification and evaluation by the Supervisory Board and the Head of the department responsible for managing Human Resources, with the latter being responsible for the actual application of the disciplinary measures outlined herein, following a report by the Supervisory Board and consultation with the hierarchical superior of the person responsible for the reprimanded conduct.

5.2.3 Measures against executives

Any conduct in breach of this Model, including the violation of the obligations to provide information to the Supervisory Body and of the principles established in the Code of Ethics, or the adoption, in the performance of activities connected with Sensitive Processes, of a conduct that does not comply with the prescriptions of the Model itself, if committed by executives, may result in the loss of the relationship of trust, with the application of the most suitable sanctions, in compliance with the provisions of Article 2119 of the Italian Civil Code and of the CCNL Metalworkers/Journalists applied to executives by the Company.

The following sanctions may be imposed on executive personnel:

- (a) verbal or written reprimand;
- (b) suspension from work
- (c) early termination of employment.

The ascertainment of any violations, as well as inadequate supervision and failure to promptly inform the Supervisory Body, will result in the precautionary suspension from work for executives, without prejudice to the executive's right to remuneration, as well as, also on a provisional and precautionary basis for a period not exceeding three months, the assignment to different tasks in compliance with Article 2103 of the Italian Civil Code.

In cases of serious violations, the Company may arrange for early termination of the employment contract without notice pursuant to and for the purposes of Article 2119 of the Italian Civil Code.

5.2.4 Measures against employees subject to management or supervision

Failure to comply - by collaborators subject to the management or supervision of the Company - with the provisions and procedures laid down in the Model, including violation of the obligations to provide information to the Supervisory Body, and with the principles laid down in the Code of Ethics, shall result, in accordance with the provisions of the specific contractual relationship, in the termination of the respective contract, without prejudice to the Company's right to claim compensation for damages suffered as a result of such conduct, including damages caused by the application of the sanctions laid down in the Decree.

5.2.5 Measures against Directors

In the event of conduct in violation of this Model on the part of one or more members of the Board of Directors, the Supervisory Body shall inform the Board of Directors and the Board of Statutory Auditors, who shall take appropriate measures depending on the seriousness of the violation observed and in accordance with the powers provided for by current legislation and the Articles of Association, including, for example, calling a shareholders' meeting in order to adopt the most appropriate measures permitted by law.

On the other hand, in case of alleged violations by the entire Board of Directors, the Supervisory Body will inform the shareholders directly and in writing.

In particular, in the event of a violation of the Model by one or more directors, the Board of Directors may, depending on the extent and seriousness of the violation, impose a formal written reprimand, temporary suspension from office or revocation, even partial, of the powers delegated and the powers of attorney conferred.

5.2.5 Measures against Auditors

In the event of conduct in violation of this Model on the part of one or more Auditors, the Supervisory Body shall inform the entire Board of Auditors and the Board of Directors, which shall take appropriate measures in relation to the seriousness of the violation observed and in accordance with the powers provided for by current legislation and the Articles of Association, including, for example, calling a shareholders' meeting in order to adopt the most appropriate measures provided for by law.

5.2.6 Measures against Service Companies, Consultants and Partners

Any conduct in violation of this Model on the part of Service Companies, Consultants, also those having a coordinated collaboration relationship, and Partners, with regard to the rules applicable to them, or the commission of Offences, shall be sanctioned in accordance with the provisions of the specific contractual clauses included in the relevant contracts.

In particular, the violation of the prescriptions and principles established in the Model and in the Code of Ethics by agents and other subjects having contractual, commercial or partnership agreements with the Company, as well as by professionals and Consultants having contractual relationships with the Company, shall determine, in compliance with the provisions of the specific contractual relationship, the right for the Company to terminate said contract *ex Article 1456 Italian Civil Code*, without prejudice to the right of the Company to claim compensation for damages resulting from such conduct, including damages caused by the application of the sanctions provided for by the Decree.

5.2.7 Measures against the Supervisory Body and other subjects

The system of disciplinary and contractual sanctions, as identified above, will also apply to the Supervisory Body or to those individuals, Employees or Directors, who, as a result of negligence, imprudence and inexperience, have failed to identify, and consequently eliminate, conduct in breach of the Model.

SECTION VI – THE MODEL

6.1 General Control Environment

6.1.1 The Company's organizational system

The Company's organizational system shall comply with the fundamental requirements of formalization and clarity, communication, and segregation of roles, especially with regard to the assignment of responsibilities, representation, definition of hierarchical lines and operational activities.

The Company shall have organizational tools (organization charts, organizational communications, procedures, etc.) based on general principles of conduct, as further detailed in paragraph 6.1.3 below:

- knowledge within the Company;
- clear and formal delimitation of roles and functions;
- clear designation of reporting lines.

Internal procedures must be characterized by the following elements:

- segregation, within each process, between the person who initiates it (decision-making impulse), the person who executes and concludes it and the person who controls it;
- written traceability of each relevant step in the process;
- adequate level of formalization.

6.1.2 The delegation and proxy system

The system for assigning Company powers and proxies is an integral part of the internal control system and represents, from the point of view of the Model, an effective means to prevent the crimes mentioned in the Decree.

The definition of criteria for the assignment of powers and proxies is up to the Board of Directors.

The system of proxies and powers of attorney must constitute:

- a) a management tool enabling the performance of acts having external or internal relevance required for the pursuit of the Company's objectives, that is consistent with the managerial responsibilities assigned to each subject;
- b) a prevention factor against the abuse of the functional powers assigned, through the definition of economic limits for each act or series of acts;
- c) an undisputable evidence to trace back corporate acts, having external or internal relevance, to the individuals who adopted them. The usefulness of the system depends on this, both in preventing the commission of Offences and in subsequently identifying the individuals who have adopted acts that are directly or indirectly connected to the commission of the Offence.

The Company's policy provides that only persons with formal and specific powers may accept commitments towards third parties in the name of and on behalf of the Company itself.

In this context, the Company has implemented a system of proxies consistent with the organizational responsibilities, entailing an effective need for representation and with the provision, when appropriate, of a precise indication of quantitative expenditure thresholds established by internal Company measures.

The Company units concerned, possibly with the support of the Supervisory Body, periodically check the system of powers of attorney in force, also by examining the documentation showing the activities actually carried out by the persons operating on behalf of the Company, suggesting any amendments if the management and/or qualification functions do not match the powers of representation conferred.

6.1.3 General principles of conduct

The organization of the Company's activities is based on compliance with the following general principles:

- (a) explicit formalization of the rules of conduct, through:
 - a clear, formal and understandable description and identification of the activities, tasks and powers attributed to each function and to the various professional qualifications and roles
 - a description of control activities and their traceability.
- b) precise definition of roles and responsibilities:
 - the internal regulations must outline the roles and responsibilities of the organizational units at all levels, homogeneously describing the activities of each structure;
 - these rules shall be made available and known within the organization;
- c) segregation of duties:
 - within each relevant Company process, the functions or persons in charge of a decision and its implementation must be separated from those who record it and those who control it;
 - there must be a clear definition of the signatory powers as well as instruments for verifying the powers exercised (for example, proxies and powers of attorney);
 - there must be no subjective identity between those who take or implement decisions, those who prepare accounting evidence of the transactions that have been agreed and those who are required to check these transactions in accordance with the law and the procedures laid down by the internal control system;
 - a precise definition of spending limits must be provided, as well as instruments for controlling spending powers (by means of, for example, authorizations and proxies).
- d) control and enforceability:
 - operational controls and their characteristics (responsibilities, evidence, frequency) must be formalized as part of procedures or other internal regulations;
 - control over the correctness of the activities carried out by the various Company departments must be guaranteed (for example, correct filing, control over the correct use of spending and signing powers);
 - documents that are important for performing sensitive activities must be suitably formalized and bear the date of filling in, acknowledgement of the document and the recognizable signature of the person filling in/supervising the document; they must be filed in places that are suitable for their storage, so as to protect the confidentiality of the data they contain and avoid any damage, deterioration or loss;
 - it must be possible to reconstruct the formation of the acts and the related authorization levels, the development of the operations, both material and registration, with evidence of their motivation and cause, in order to guarantee the transparency of the choices made;
 - the adoption of IT systems must be envisaged, where possible, to guarantee the correct and truthful attribution of each operation, or of a segment thereof, to the person responsible for it and to the subjects taking part in it. The system must provide for the impossibility to modify the records;

- documents concerning the Company's activities, and in particular computer documents relating to sensitive activities, shall be filed and stored in such a way as not to allow any subsequent modification, unless specifically recorded;
- access to documents already filed must always be justified and allowed only to persons authorized according to internal rules or to a delegated person, to the internal control bodies, to the Auditing Firm and to the Supervisory Body.

(A) Relations with Service Companies/Consultants/Partners: general principles of conduct

Relations with Service Companies/Consultants/Partners, within the framework of Sensitive Processes and/or At-Risk Activities of Offence shall be characterized by the utmost fairness and transparency, compliance with the provisions of law, the Code of Ethics, the Model and the internal Company procedures, as well as the specific ethical principles on which the Company's business is based.

Service Companies, Consultants, commercial agents, suppliers of products/services and, in general, Partners (e.g. temporary business association) must be selected according to a specific procedure which takes into account the following aspects:

- verify the **commercial and professional reliability** (e.g. through the verification of the Chamber of Commerce documents to ascertain the consistency of the activity performed with the services requested by the Company, a self-certification pursuant to D.P.R. 445/00 concerning any pending charges or sentences issued against those who hold administrative, management or control functions within the counterparty in question);
- verify and monitor that the commercial counterparts are not involved in actions that may entail the risk of committing Offences such as corruption, money laundering and/or financing of terrorist activities, or cause a potential involvement, even involuntary, of the Company in such actions with a consequent serious reputational damage;
- select an offer on the basis of quality, innovation, costs and sustainability standards, with particular reference to respect for human rights and workers' rights, the environment, and the principles of legality, transparency and correctness in business (this qualification process must provide for high quality standards that can also be verified through the acquisition of specific quality certifications);
- avoid any commercial and/or financial transaction, whether direct or through an intermediary, with individuals or legal entities that are involved in investigations by the judicial authorities for alleged Offences and/or have been reported by European and international organizations and authorities responsible for preventing terrorist, money laundering and organized crime Offences
- avoid/not accept contractual relations with subjects - natural persons or legal entities - who have their headquarters or residence or any connection with countries considered uncooperative because they do not comply with the standards of international laws and the recommendations expressed by FATF-GAFI (Financial Action Group against money laundering) or which are included in the prescription lists (so-called "Black Lists") of the UN, the European Union, OFAC (Office of Foreign Assets Control) and the World Bank;
- pay fees only if properly justified in the context of the contractual relationship established or in relation to the type of assignment to be carried out and in accordance with local practices;
- not make any payments in cash and, in exceptional cases, obtain appropriate authorization. In any case, payments must be made in accordance with appropriate administrative procedures proving the traceability of the expense;

- with reference to financial management, the Company implements specific procedural controls and pays close attention to flows that do not form part of the Company's typical processes and are therefore managed in an extemporary and discretionary manner. These controls (e.g. frequent reconciliation of accounting data, supervision, segregation of duties, juxtaposition of functions, in particular the procurement and financial functions, an adequate system documenting the decision-making process, etc.) are designed to prevent the formation of hidden reserves.

(B) Relations with service companies/Consultants/Partners: Contractual clauses

Contracts with service companies/Consultants/Partners shall provide for the formalization of specific clauses that

- regulate the commitment to comply with the Code of Ethics and with the Decree adopted by F2M eSolutions, as well as provide a declaration relating to the absence of any involvement in legal proceedings relating to the Offences set forth in the Decree (or, if positive, a declaration for the purposes of a greater attention on the part of the Company in the event the consultancy or partnership relationship is established). This commitment may be mutual, if the counterpart has adopted its own and similar code of conduct and model;
- define the consequences of violating the rules of the Model and/or the Code of Ethics (e.g. express termination clauses, penalties);
- regulate the commitment, for foreign service companies/Consultants/Partners, to conduct their business in compliance with rules and principles similar to those provided for by the laws of the State (or States) where they operate, with particular reference to crimes of corruption, money laundering and terrorism and to the rules that provide for the liability of legal persons (Corporate Liability), as well as the principles contained in the Code of Ethics, aimed at ensuring compliance with adequate levels of ethics in their business activities;
- allow the Company or individuals/entities delegated by it, consistently with the type of contract, to carry out inspections, checks and controls concerning the performance of the activities covered by the contract, as well as to provide for final testing of the purchased goods.

(C) Relations with Customers: general principles of conduct

Relations with customers must be based on the utmost fairness and transparency, in compliance with the Code of Ethics, the Model, the law and internal Company procedures, which take into account the following aspects

- accepting payments in cash (and/or other untraceable methods) only to the extent permitted by law;
- grant extensions of payment only if solvency has been ascertained;
- refuse sales in violation of international laws/regulations, restricting the export of products/services and/or protecting the principles of free competition;
- charge prices in line with average market values (except for commercial promotions and any donations, provided that both are adequately justified/authorized).

6.1.4 Specific control standards

It is forbidden to engage in conduct that may be construed as a Predicate Offence as indicated in each Special Section, or conduct that, although not necessarily constituting an Offence in itself, may potentially

be construed as one of the Offences examined in the Special Sections. Each section of the Special Section contains rules of conduct relating to processes that are most exposed to the risk of committing Predicate Offences.

6.1.5 Financial flow management system

In line with the requirements of the Reference Guidelines, the Company adopts a system for the management of financial flows based on the principles of transparency, verifiability and relevance for the Company's business, using mechanisms to cover decisions through procedures that document and verify the various stages of the decision-making process, in order to prevent the improper management of the Company's resources.

Correct management of the process, also in accordance with the provisions of Article 6, paragraph 2, letter c) of the Decree, contributes to preventing the risk of multiple Offences being committed by the Company.

With regard to the management of financial flows, the Company applies the following control principles

- segregation of duties in the key phases/activities of the process (e.g. authorization, reconciliation);
- system of delegated and proxy powers constantly aligned with the authorization profiles stored in the IT systems;
- system of internal practices/procedures governing the main processes on which financial flows impact;
- adequate traceability of information and document flows.

6.2 F2M eSolutions Sensitive Processes

The risk analysis carried out by F2M eSolutions for the purposes of the Decree, as detailed in paragraph 3.1.3, has shown that the Sensitive Processes at present mainly concern the following Offences:

- 1) crimes against the PA and crimes against the Administration of Justice;
- 2) Cyber crimes;
- 3) Organized crime Offences;
- 4) Offences of falsification of instruments or signs of recognition and Offences against industry and commerce;
- 5) Corporate Offences;
- 6) Offences with the purpose of terrorism and subversion of the democratic order;
- 7) Crimes against the individual;
- 8) Market abuse Offences;
- 9) Crimes of negligent homicide and serious or very serious negligent injury, committed in violation of the rules on accident prevention and the protection of hygiene and health at work;
- 10) Offences of fencing, money laundering and use of money, goods or utilities of unlawful origin, as well as self-laundering;
- 11) Offences relating to the violation of copyright;
- 12) Environmental Offences;
- 13) Tax Offences;

With regard to the following Offences provided for by the Decree

- a) Counterfeit currency, with the exclusion of the Offences referred to in articles 473 and 474 of the Italian Criminal Code;
- b) Crimes against the individual (slavery and child pornography);
- c) Mutilation practices of female genital organs;
- d) Sports fraud,

it is believed that - in view of the Company's business and the context in which it operates - the risk of these Offences is negligible, if not non-existent and, therefore, without prejudice to the reference to conduct that complies with the relevant regulations, as well as to the general rules of conduct set out in the Model and in the Code of Ethics, it was not deemed necessary to create a specific section in the Model, nor to establish specific controls.

Details of the types of Offences listed above are given in **ANNEX A: Types of Predicate Offences**.

The objective of this Section is to

- outline the principles and procedures that Employees, Corporate Bodies, Service Companies, Consultants and Partners of F2M eSolutions are required to observe in order to effectively prevent the risk of committing Offences when carrying out activities in which the risk of committing one of the aforementioned Offences is conceivable;

- provide the Supervisory Body and the heads of the other Company departments that cooperate with it with the executive tools to exercise control, monitoring and verification activities through the procedures in force and being issued by the Company.

A. Sensitive Processes in criminal offenses against the Public Administration and against the Administration of Justice

The main Sensitive Processes and Instrumental Activities that the Company identified internally in relation to the Offences set forth in Articles 24, 25 and 25-*decies* of the Decree are as follows:

Sensitive Processes	At-Risk Activities	Predicate Offence ¹
Participation in tender or direct negotiation procedures issued by Italian or foreign public bodies for the assignment of orders	<p>Communications concerning a contract stipulated or to be stipulated between the Company and the PA;</p> <p>Determining the value of the asset covered by the contract between the Company and the PA;</p> <p>PA review of compliance with contractual agreements;</p>	Articles 24, 25 and 25- <i>decies</i> of the Decree
Management of relations with the PA	<p>Acquisition and management of orders assigned by the PA;</p> <p>Management of institutional relations with subjects belonging to the PA;</p> <p>Management of inspections (administrative, tax, social security, etc.).</p>	Articles 24, 25 and 25- <i>decies</i> of the Decree
Requesting and obtaining public funding		Articles 24, 25 and 25- <i>decies</i> of the Decree
Managing donations/sponsorships and gifts		Articles 24, 25 and 25- <i>decies</i> of the Decree

Furthermore, within the context of the type of Offence related to Article 25 "Corruption and Extortion" of the Decree, the following Core Activities have been identified:

- bestowing gifts or gratuities;

¹ For a detailed description of the individual Offences and their sentencing, see Annex A.

- recruitment promises and *rewarding* system;
- managing Consultants/supplies;
- concession and use of goods or services typical of the Company;
- sponsorships;
- expense reimbursements;
- liquidity and cash flows management in general.

The general criteria for the definition of Public Administration and, in particular, of Public Official and of Person in Charge of a Public Service, are set out in **ANNEX A: Types of Predicate Offences**

This definition includes a wide category of subjects with whom the Company may have to operate in performing its activities. It includes not only Public Bodies, and those who perform a legislative, judicial or administrative public function (Public Officials), but also persons/entities entrusted by the PA, e.g. through an agreement and/or concession, and irrespective of the legal nature of the person/entity, which may also be governed by civil law - with the assumption of public interests or the satisfaction of needs in the general interest (public service appointees). Not all natural persons acting within the sphere of the above-mentioned entities and in relation to them are persons in respect of whom (or by whom) Offences are committed in relations with the PA.

In particular, the figures relevant for this purpose are only:

- "Public Officials" and
- "Persons in Charge of a Public Service".

According to Article 357, first paragraph, of the Italian Criminal Code, a Public Official is "*for the purposes of criminal law*" whoever exercises "*a legislative, judicial or administrative public function*". The provision only clarifies the concept of "public administrative function" (the other two did not raise doubts as to their interpretation) by stating that, for the purposes of criminal law, "an administrative function is public if it is governed by rules of public law and acts of authority and is characterized by the formation and manifestation of the will of the public administration or its exercise by means of powers of authority or certification".

In other words, an administrative function is defined as a public function that is governed by "public law rules", *i.e.* rules that pursue a public purpose and protect a public interest and, as such, are opposed to private law rules.

In contrast, Article 358 of the Criminal Code defines "*persons entrusted with a public service*" as those "*Who, for whatever reason, provide a public service. The term 'public service' is to be understood as referring to an activity governed in the same way as a public function, but characterized by the absence of the powers characteristic of the latter, and excluding the performance of mere orderly tasks and the execution of purely material work*".

Lawmakers have clarified the concept of "public service" by means of two sets of criteria, one positive and one negative. In order for the service to be defined as public, it must be governed, like "public office", by public law rules, but in the absence of the certification, authorization and decision-making powers of the public office.

A person in charge of a public service is therefore a person who performs a public function which does not fall within the powers of a public official (legislative, judicial and administrative powers) and which does not

relate to mere orderly tasks and/or the performance of purely material work, insofar as there is no intellectual or discretionary contribution.

Rules of conduct

In the exercise of their respective activities and functions, in addition to the knowledge of and compliance with the rules, established in the Company Articles of Association, the principles established in the Code of Ethics, and in the Anti-Corruption Guidelines, in the Company's policies, as well as what is set out in the "**General Control Environment**" paragraph at the beginning of this section, the Recipients of the Model who, in any capacity, have relations with Public Officials, Persons in charge of a Public Service or, more generally, with the Public Administration, in the name and on behalf of the Company, must comply with the following general rules of conduct in order to effectively prevent the risk of committing Offences against the Public Administration and against the Administration of Justice:

- verify that the Employees acting in the name of and/or on behalf of the Company in the process of applying for subsidized loans from public bodies are formally identified and delegated;
- make truthful statements to national or EU public bodies in order to obtain grants, contributions or funding;
- provide a reporting account of the actual use of the funds obtained through public contributions and financing;
- carry out procedural controls with reference to financial management, with particular attention to flows that do not fall within the Company's typical processes and are therefore managed in an extemporary and discretionary manner, in order to prevent the formation of hidden reserves;
- verify that the persons participating in judicial, tax and administrative inspections (e.g. relating to Legislative Decree 81/2008, tax audits, INPS, etc.) are expressly identified and that the appropriate minutes are drawn up and kept;
- do not distribute gifts and gratuities outside the provisions of the Company's procedures and the Code of Ethics: permitted gifts are always characterized by their low value or because they are intended to promote charitable or cultural initiatives or the Company's brand image. Gifts offered - except those of modest value - must be properly documented. In particular, it is forbidden to make any gift to Italian or foreign public officials or their relatives that could influence their independence of judgement or induce them to secure any advantage for the Company;
- do not promise or make money donations, even through third parties, and do not grant advantages of any kind (recruitment promises etc.) to Italian or foreign public officials, either directly by Italian entities or their employees, or through persons acting on behalf of such entities both in Italy and abroad, in order to obtain benefits for the Company;
- do not influence, through promises or the granting of advantages of any kind, in the course of any business negotiation, request or relationship with the PA, the decisions of officials who negotiate or make decisions on behalf of the PA;
- do not grant any compensation, offer or promise advantages of any kind to Employees/clients/suppliers/Partners/service companies that are not adequately justified in the context of the work or contractual relationship established with them and in accordance with current local practices;

- do not offer corporate hospitality (including meals and entertainment) to public officials outside the provisions of Company procedures and the Code of Ethics: business and work relations must take precedence over entertainment, which must not be excessive and must be offered only as an accessory;
- do not be represented in dealings with the PA, by Consultants or third parties who may create conflicts of interest;
- do not solicit and/or obtain confidential information that could compromise the integrity or reputation of either party;
- do not behave with the purpose or effect of inducing a person to make false statements before the Judicial Authority;
- in relations with Public Authorities, in particular with judicial and investigative Authorities, maintain a clear, transparent, diligent and collaborative behaviour, providing all information, data and news that may be requested;
- do not breach the PA's information systems in order to obtain or manipulate information to the Company's advantage;
- do not carry out any operation aimed at creating non-accounting funds.

Furthermore:

- a) Managers are responsible for training and updating their Employees and collaborators. In particular, managers are required to (i) circulate the Company's ethical principles defined in the Code of Ethics, (ii) promote the principles of transparency and organizational clarity among Employees in order to foster their accountability and contribute to the achievement of the planned objectives, (iii) inform on the rules of conduct and standards required by the Company in its relations with the Public Administration, (iv) ensure that each Employee participates in and undergoes training on the issues set forth in the Decree;
- b) Company Employees who make payments or, in general, transactions with the PA and/or foreign public officials, should be aware of the specific rules of conduct established in this model and in the Code of Ethics to counter attempts at corruption;
- c) All business Partners of the Company must be informed about the anti-corruption rules of conduct prepared by the Company;
- d) Any critical issues or conflicts of interest arising in the relationship with the PA should be reported to the hierarchically superior business function.

B. Sensitive Processes in cybercrime Offences

The main Sensitive Processes that the Company has concretely identified within its own organization, in relation to the Offences set forth in Article 24-*bis* of the Decree, are the following:

Sensitive Processes	At-Risk Activities	Predicate Offence ²
Computer/Telematics System Management	Installation/maintenance of computer equipment (<i>software</i> and <i>hardware</i>). Monitoring access to computer/telematics systems.	Article 24 <i>bis</i> of the Decree
Use of computer/telematics systems to support work activities	Access to external computer/telematics systems.	Article 24 <i>bis</i> of the Decree

The risk of committing the Offences referred to in this section may materialize, to a greater extent, in those areas (activities, functions, processes) in which staff, in carrying out their activities, have at their disposal an IT system with external connectivity and, in particular, the IT area, given the specific skills and knowledge of Employees working in this field.

Specific principles of conduct

Further to the contents of the paragraph "**General Control Environment**", at the beginning of this section, a number of additional principles of conduct are listed below, which must be complied with specifically in order to effectively prevent the risk of commission of cybercrime Offences:

- provide the Recipients with adequate information on the correct use of corporate IT resources and on the risk of committing cybercrime Offences;
- do not disclose information relating to the Company's IT systems;
- limit access through corporate resources to external computer systems and networks compatibly with work requirements;
- carry out, in compliance with privacy regulations, standing trade union agreements and the Workers' Statute, periodic checks of the Company's IT network in order to identify anomalous behaviour such as, for example, the *downloading* of large *files*, or exceptional activities of the *servers* outside the Company's operating hours;
- set up and maintain adequate physical defences to protect the Company's *servers* and, more generally, to protect all the Company's IT system, including through the setting up of a system to control access to the *server* rooms, providing, where possible, controls to prevent the entry and exit of unauthorized material;

² For a detailed description of the individual Offences and their sentencing, see Annex A.

- adequately inform users of IT systems of the importance of keeping their access codes (*username* and *password*) confidential and not disclosing them to third parties;
- distribute to the users of IT systems a specific document in which they undertake to use the Company's IT resources correctly;
- inform users of IT systems of the need not to leave their computer systems unattended and the convenience of locking them, should they leave their workstation, with their own access codes;
- set up the IT systems themselves in such a way that, if they are not used for a certain period of time, they automatically shut down;
- access from and to the outside (Internet connection) must be authorized and carried out only in the authorized manner;
- equip the servers room with a door with a physical access control allowed only to authorized personnel;
- protect every Company computer system, in order to prevent the unlawful installation of *hardware* devices capable of intercepting communications relating to a computer or telematics system, or between several systems, or capable of preventing or interrupting them;
- provide each computer system with appropriate firewall and anti-virus software and ensure that, where possible, these cannot be disabled;
- prohibit the installation and use of software (programs) not approved by the Company and not related to the professional activity carried out by the Recipients or users;
- limit access to particularly sensitive areas and Internet sites that are particularly sensitive as they are vehicles for the distribution and dissemination of infected programs (so-called "viruses") capable of damaging or destroying computer systems or data contained therein (for example, e-mail sites or sites for disseminating information and *files*);
- prohibit, in particular, the installation and use, on the Company's computer systems, of *software* (so-called "*P2P*", *file sharing* or unauthorized *instant messaging*) through which it is possible to exchange with other subjects within the Internet network all types of *files* (such as films, documents, songs, viruses, etc.) without any possibility of control by the Company;
- protect the *wireless connections* (*i.e.* without wires, by means of *routers* equipped with Wi-Fi antennae), possibly used to connect to the network, by setting an access key, in order to prevent third parties, external to the Company, from illegally connecting to the Internet network through the *routers* of the same and committing Offences ascribable to Company's Employees;
- provide, where possible, an authentication procedure by means of username and password which corresponds to a limited profile of the system resources management, specific to each recipient or category of recipients.

Cybercrimes also include so-called misrepresentations. It is therefore absolutely forbidden to transmit any untruthful, forged or inauthentic document by electronic means.

C. Sensitive Processes in organized crime Offences

The organized crime Offences envisaged by Article 24-ter of the Decree and by Articles 3 and 10 of Law no. 146/2006 imply the existence:

- of a stable associative bond between three or more persons, intended to last even beyond the commission of the Offences actually planned;
- of a criminal program aimed at committing an indeterminate number of crimes;
- of an organizational structure adequate to accomplish criminal objectives.

Therefore, the liability of the Entity extends to any type of Offence carried out in the form of an association, regardless of the actual commission of the Offence-aim, even if not directly included in the scope of application of the Decree.

The Company believes that it must monitor the internal organization by means of a suitable separation of duties and the processes for managing relations with suppliers/customers/Partners, through specific controls on the following Risk Activities:

At-Risk Activities	Predicate Offence ³
Qualification and selection of suppliers/clients/Partners	Article 24 ter of the Decree
Contractual relations/investments	
Management of payments/collections made/received	
Filling, keeping, storing and preparing accounting records and related activities and managing accounting and tax obligations	

Specific principles of conduct

Further to the contents of the paragraph "**General Control Environment**", at the beginning of this section, a number of additional principles of conduct are listed below, which must be complied with specifically in order to effectively prevent the risk of committing organized crime Offences at national and transnational level:

- provide for adequate segregation of duties and responsibilities in the management of the supplier/Partner, with particular reference to the evaluation of offers, the execution of the service and its approval, as well as the settlement of payments;
- verify the regularity of payments, with reference to the full correspondence between the recipients/payment orderers and the counterparties actually involved in the transactions;

³ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

- carry out formal and substantial controls on corporate cash flows, with reference to payments to third parties. These controls shall take into account the registered office of the counterparty company (e.g. tax heavens, countries at risk of terrorism, etc.), banking institutions (registered office of the banks involved in the transactions and institutions that do not have physical establishments in any Country) and any corporate shields and trust structures used for extraordinary transactions or operations;
- do not receive financing from individuals, companies or organizations convicted of having carried out terrorist or public order subversion activities, whether they are companies under Italian or foreign law, included in the so-called "Country Lists" and/or with natural or legal persons indicated in the so-called "Nominative Lists" (hereinafter referred to jointly as the "Lists") linked to international terrorism available on the Bank of Italy's website;
- do not make monetary donations to individuals, companies or organizations convicted of illegal activities, in particular terrorist or public order subversion activities;
- do not have contacts with individuals on searchable anti-terrorism blacklists available at <http://www.consilium.europa.eu/it/policies/fight-against-terrorism/terrorist-list/>.

D. Sensitive Processes within the context of Offences of falsification of instruments or signs of identification (counterfeiting, alteration or use of trademarks or distinctive signs or of patents, models and designs) and Offences against industry and commerce.

The analysis of corporate processes led to the conclusion that the risk of committing Offences against industry and trade, pursuant to Article 25-*bis*-1 is very low, as they do not relate to the Company business, or it is not possible to assume that these offences may be committed and, in any event, they are already covered by the rules of conduct laid down in the Code of Ethics.

Therefore, the main Sensitive Processes the Company identified internally in relation to the Offences set forth in Articles 25-*bis* and 25-*bis* 1 of the Decree are the following:

Sensitive Processes	At-Risk Activities	Predicate Offence ⁴
Industrial product development	<i>Co – design</i> product development	Articles 25- <i>bis</i> and 25- <i>bis</i> 1 of the Decree
Creation and dissemination of advertising and promotional initiatives	Organization of promotional events directly or through external Consultants and suppliers.	

Specific principles of conduct

The Company demands and requires respect for its own and third parties' industrial property rights and trade secrets. In particular, in-house knowledge is a fundamental resource that every employee and recipient must protect. In the event of improper disclosure or violation of the rights of third parties, the Company may suffer damage to its assets and image. Consequently, disclosure to third parties of information concerning the Company's technical, technological and commercial knowledge is prohibited, except in cases where such disclosure is required by judicial authorities, laws or other regulations, or where it is expressly provided for in specific contractual agreements with which counterparties have undertaken to use such information exclusively for what it is intended and to maintain its confidentiality.

Moreover, the Company takes an active part in tackling the counterfeiting of its brands and products, using all the tools made available by the legislative systems where the Company operates, in particular by cooperating with the Authorities in charge of combating such crimes, through agreements, training meetings (e.g.: Customs Authorities in charge of intercepting counterfeit goods).

In addition to what reported in paragraph "**General Control Environment**", at the beginning of this section, some additional principles of conduct are listed below, which must be specifically complied with for an effective prevention of the risk of committing the Offences in question.

(i) **With regard to product and process innovations**, the following behavioral principles are specified:

- avoid, by means of preventive checks, possible implementations of solutions covered by third parties' patents and in particular:

⁴ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

- monitor *competitors* operations, identifying technological development lines, analyzing public patents of leading companies with the aim of reducing the risk of infringement of third party rights;
 - provide for a periodic patent surveillance system;
- guarantee, starting from *concept* selection phase, the implementation of the most appropriate protective measures;
 - carry out timely and effective searches by consulting specialized databases or with the support of external Consultants;
 - check for the presence of patents so that the product does not infringe them (so-called "freedom to operate or implement");
 - check for patents that have expired and related technology that is now in the public domain;
 - evaluate possible rights that could be abandoned as a result of changes in the state of the art, through periodic meetings also dedicated to reviewing the so-called "intangible" portfolio;
 - provide for the use of the secrecy agreement in all cases of technical collaboration, including exploratory and study collaboration with third parties, so as to avoid that disclosure of ideas not adequately protected and documented can render any subsequent patent null and void or allow third parties to claim paternity in advance;
 - define policies or operational instructions which allow, in coordination with the consulting firms, to document the authenticity of the invention (updated, signed, dated registers, etc.) in case of litigation;
 - define a policy for the use of technical solutions covered by the exclusive rights of third parties and for the consequent stipulation of licenses or concessions;
 - monitor intellectual property management **clauses** in contracts and licenses. In particular, in case of co-design agreements or contracting out product development to third parties, the Company shall:
 - provide, in collaboration contracts, clauses defining the ownership of technical results of the work under agreement, in particular models, prototypes, simulacra, technical or technological documentation, know-how, inventions, innovations, up-grades, *software*, simulation models;
 - envisage the possibility of proceeding with the registration of the results as patents, ornamental or utility models with the commitment of the parties involved and their Employees to collaborate during the relative filing, prosecution and territorial extension procedures;
 - explicitly request that any result of the design activities entrusted based on the agreement, does not involve any infringement of intellectual property rights of third parties so that the Company may have free, unconditional and exclusive availability of all intellectual property rights to be able to use freely for the production and marketing of the product without any dispute by the same supplier and / or third parties in all states identified by the parties for the purpose of explicit protection;
 - provide that the supplier/Partner who need to use some technical solution for which a third party holds related intellectual property rights, shall inform the Company in advance if they

intend to use such solution, obtaining, at their own expense, a license to use it from the party holding said intellectual property rights;

- provide that, in the event of a dispute by third parties, on the use of special products designed independently by the supplier/Partner, the latter indemnifies and holds harmless the Company from any claim, damage and/or any measure that may limit the production and/or sale of the product by the Company, to the extent that they deem most appropriate;
 - provide for confidentiality obligations towards the supplier/Partner, so that they treat as confidential all technical information received by the Company and do not use, for activities other than those referred to in the agreement, information of any kind relating to the activities carried out, of which they become aware during the period of validity of the agreement;
- identify the Corporate body responsible for defending the claims made by third parties regarding the unauthorized use of their property rights.

(ii) **With regard to the characteristics of the product marketed**, the following behavioural principles are specified:

- the Company considers it essential that its customers be treated fairly and honestly and therefore requires its managers, other Employees and Recipients of the Model to ensure that all relations and contacts with customers are based on honesty, professional correctness and transparency;
- in the relationship with customers, Employees must follow internal procedures aimed at achieving the set objectives also through the maintenance of profitable and lasting relationships with customers, offering assistance and professional support;
- Contracts with suppliers/Partners must contain special clauses in which they undertake to guarantee that the quality of the products covered by the contract is compliant with
 - what provided for by the technical standards in force at the Company, by every legal, regulatory, administrative provision or jurisdictional or administrative measure applicable or to be applied in the countries in which the product is to be marketed;
 - standards, specifications, rules, bulletins, procedures and other similar regulations, from time to time communicated or made known to the supplier/Partner;
- contracts with the supplier/Partner shall contain specific clauses allowing the Company or its authorized persons/entities to carry out inspections, checks and controls of the production processes, means of production, processing methods and/or control and testing methods including, *inter alia*, any control and/or inspection concerning the fulfilment of requirements for product certification/approval.

E. Sensitive Processes in corporate crimes

Corporate crimes laid down in Article 25-ter of the Decree are proper Offences and, as such, can be committed by:

- Board of Directors;
- Administrators;
- General Managers;
- Liquidators;
- Individuals subject to the direction and supervision of the subjects listed above (in case of corruption amongst private individuals);

as well as, by way of conspiracy, also by structures in charge of administrative-accounting management, financial activities or relating to the implementation of the accounting IT system.

The main Sensitive Processes the Company identified internally in relation to the crimes set forth in Article 25-ter of the Decree are the following:

Sensitive Processes	At-Risk Activities	Predicate Offence ⁵
Preparation of communications to shareholders and/or third parties relating to the Company's economic, equity and financial situation (e.g. financial statements accompanied by the relevant reports required by law)	Preparation of the Balance Sheet, Income Statement, Notes to the Financial Statements and Report on Operations.	Article 25-ter of the Decree
Management of control activities by Shareholders, the Board of Statutory Auditors and the Auditing Firm	Control carried out by the Shareholders, the Board of Statutory Auditors and the Auditing Firm.	Article 25-ter of the Decree
Management conflicts of interest	Reporting conflicts of interest.	Article 25-ter of the Decree
Management of relations with suppliers/customers/Partners	Qualification and selection of suppliers/clients/Partners. Contractual relations/investments. Management of payments/collections made/received.	Article 25-ter, paragraph 1, lett. s-bis of the Decree

Furthermore, within the scope of this type of crime, the following Instrumental Activities have been identified:

- giving gifts or gratuities;

⁵ For a detailed description of the individual Offences and the relevant sentencing, see Annex A.

- promises of employment;
- management of consultancies/supplies;
- granting and using goods or services typical of the Company;
- sponsorships;
- reimbursement of expenses.

Specific principles of conduct

In addition to what stated in the paragraph "**General Control Environment**", at the beginning of this section, some additional principles of conduct are listed below, which must be observed specifically for effective prevention of the risk of committing corporate Offences.

This Section also provides for the express obligation of the Company's Corporate Bodies, Employees and Consultants, to the extent necessary for the functions performed by them, to

- pursue the objective of the Company's interest in the management and exercise of the Company's activities, up to the eventual phases of liquidation or termination of the Company;

(i) As part of the preparation of communications to shareholders and/or third parties relating to the Company's economic, equity and financial situation (e.g. financial statements accompanied by the relevant statutory reports):

- comply with the principles and requirements for the preparation of financial statements and periodic reports governed by law;
- behave in a correct, transparent and collaborative manner, in compliance with the law and internal Company procedures, in all activities aimed at preparing the financial statements and other Company communications, in order to provide shareholders and third parties with true and correct information on the Company's economic, equity and financial situation (it is forbidden to, by way of example, represent or transmit for the preparation and representation of financial statements, reports and prospectuses or other corporate communications, false, incomplete or in any case untrue data on the economic, asset and financial situation of the Company, or omit data and information required by law on the economic, asset and financial situation of the Company);
- strictly observe all the rules laid down by law to protect the integrity and effectiveness of share capital, so as not to prejudice the guarantees of creditors and third parties in general (by way of example, it is forbidden to return contributions to shareholders or release them from the obligation to make them, except in cases of legitimate reduction of share capital; distribute profits or advances on profits that have not actually been earned or that are destined by law to reserves; carry out reductions in share capital, mergers or demergers, in violation of the provisions protecting creditors; proceed with the fictitious formation or increase of share capital);
- carry out with timeliness, correctness and good faith all the communications required by the law without hindering the controls of the Supervisory Authorities;
- draw up these documents according to specific Company procedures which:
 - determine with clarity and completeness data and information that each function must provide, the accounting criteria for processing the data and the timeframe for their delivery to the responsible functions;

- provide for the transmission of data and information to the responsible function by means of a system (also computerized) which allows the tracing of the individual steps and the identification of the persons who enter the data in the system;
- compliance with the authorization powers, proxies and powers of attorney shall be adequately monitored by the Company's supervisory bodies by means of sample-based interventions on the signed documentation;
- prepare a basic training programme on the main legal and accounting notions and issues concerning financial statements, addressed at all managers of functions involved in the preparation of the financial statements and other related documents, taking care, in particular, both of the training of new recruits and of periodic refresher courses.

(ii) As part of the Management of relations with the auditing firm:

- ensure the regular functioning of the Company and of the Corporate Bodies, guaranteeing and facilitating all forms of internal control over the management of the Company as required by law, as well as the free and correct formation of the will of the shareholders' meeting;
- comply with the Group procedure governing the appointment of the Auditing Firm;
- identify the personnel responsible for communicating with the auditing firm and for sending the related documentation;
- allow the auditing firm to contact the Supervisory Body to jointly verify situations that may present critical aspects in relation to corporate Offences;

(iii) In the context of the management of relations with suppliers/customers/Partners/intermediaries, the following behavioral principles are specified (in relation to the Offence of "Corruption amongst private individuals"):

- act strictly on the controls necessary to ensure transparency in relations with customers or other contractual counterparties;
- identify general and transparent criteria for determining a maximum bid price for each product or service, so that any anomalies can be easily detected;
- do not distribute gifts and gratuities outside the scope of Company procedures and the Code of Ethics: permitted gifts are always characterized by their low value or because they are aimed at promoting charitable or cultural initiatives or the brand image of the Company. Gifts offered - except those of modest value - must be adequately documented. In particular, any gift to suppliers/clients/Partners/intermediaries that may influence the independence of judgement or induce to secure any advantage for the Company is prohibited;
- do not make donations to charity or sponsorships without prior authorization or outside the scope of Company practice; such contributions must be intended exclusively to promote initiatives of a charitable or cultural nature or the brand image of the Company. All proposals for donations must be assessed by the Department of Legal Affairs and must receive the appropriate administrative and financial approvals;
- do not make expenditures for meals, entertainment or other forms of hospitality beyond the scope of Company procedures and the Code of Ethics;
- avoid any conflict of interest, with particular reference to interests of a personal, financial or family nature (e.g. the existence of financial or commercial shareholdings in supplier companies, customers or

competitors, improper advantages deriving from the role played within the Company, etc.), which could influence independence towards suppliers/clients/Partners/intermediaries;

- do not make monetary donations and do not grant advantages of any kind (promises of employment, etc.) to suppliers/clients/Partners either directly or through intermediaries;
- do not hire or make promises of employment that are not based on criteria of objectivity, competence and professionalism and that are not adequately documented;
- do not pay fees, commissions, offer or promise advantages of any kind to suppliers/clients/Partners/intermediaries that are not adequately justified in the context of the working relationship or contractual relationship established with them and in accordance with local practices;
- provide for adequate segregation of duties and responsibilities in management:
 - of the supplier/Partner/intermediary, with particular reference to the evaluation of offers, the execution of the service/supply and its approval, as well as the settlement of payments;
 - of the customer, with particular reference to the definition of the price, conditions and payment terms and discounts;
- any financial transaction must presuppose knowledge of the beneficiary of the sum involved;
- verify the correspondence between the contractual object and the service/supply provided, as well as the correspondence between the recipients/orderers of the payments and the counterparties actually involved in the transactions;
- provide, in the information to customers/suppliers, that any breach to the principles contained in the Code of Ethics represents a contractual violation, and the obligation to comply with the Code of Ethics before having business relations with the Company.

F. Sensitive Processes in crimes of terrorism and subversion of the democratic order

The main Sensitive Processes the Company identified internally in relation to the crimes set forth in Article 25-*quater* of the Decree are as follows

Sensitive Processes	At-Risk Activities	Predicate Offence ⁶
Negotiation/conclusion and execution of contracts/concessions with third parties through negotiated procedures	Selection of Business Partners	Article 25 <i>quater</i> of the Decree

The risk of committing the Offences contemplated in this paragraph and, in particular, the financing of terrorism may be greater in certain areas (activities, functions, processes), among which the financial and administrative departments are of central importance.

Specific principles of conduct

In addition to what is reported in the paragraph "**General control environment**", at the beginning of this section, some additional principles of conduct are listed below, which must be specifically observed for an effective prevention of the risk of committing crimes of terrorism and subversion of the democratic order:

- any financial transaction shall presuppose knowledge of the beneficiary of the sum involved;
- data collected regarding relations with customers, Consultants and Partners shall be complete and up-to-date, both for their correct and timely identification and for a valid assessment of their profile;
- always be aware of the use that will be made of Company funds managed by third parties;
- it is forbidden to carry out operations or take on orders that are considered anomalous in terms of type or subject matter and to establish or maintain relationships with anomalous profiles;
- it is forbidden to take on orders, supply products or carry out any commercial and/or financial operation, either directly or through an intermediary, with individuals or legal entities whose names have been reported by European and international authorities responsible for preventing terrorist crimes;
- proposals to donate corporate assets to charitable activities or social groups shall be evaluated by the Department of Legal Affairs and receive the appropriate administrative and financial approvals.

⁶ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

G. Sensitive Processes in Offences against the individual

The main Sensitive Processes that the Company has concretely identified internally in relation to the Offences referred to in Articles 25-*quater* 1, 25-*quinquies* and 25-*duodecies* of the Decree are as follows

Sensitive Processes	At-Risk Activities	Predicate Offence ⁷
Conclusion of contracts with employment agencies	Qualification and selection of suppliers in relation to works and procurement contracts	Articles 25- <i>quater</i> 1, 25- <i>quinquies</i> and 25- <i>duodecies</i> of the Decree
Hiring and managing staff	Use of occasional staff; Employment of personnel from non-EU countries	Articles 25- <i>quater</i> 1, 25- <i>quinquies</i> and 25- <i>duodecies</i> of the Decree
Management of websites and use of the Internet/Intranet network	Reception/dissemination of virtual child pornography material via internet/intranet	Articles 25- <i>quater</i> 1, 25- <i>quinquies</i> and 25- <i>duodecies</i> of the Decree

Specific principles of conduct

In addition to the paragraph "**General Control Environment**", at the beginning of this section, some additional principles of conduct are listed below, which must be specifically observed for an effective prevention of the risk of committing Offences against the individual:

- in the selection of suppliers (especially for particular services, such as cleaning, travel arrangements, etc.) always carefully assess their reliability, also by means of *ex ante* investigations (especially in relation to particular risk indicators such as the cost of that supplier's staff, the allocation of production facilities, etc.) and requesting any useful documents in this regard;
- establish and maintain relations with suppliers based on the utmost fairness and transparency, requesting, during the contract, guarantees that the latter will respect the rights and dignity of the workers they employ;
- in case of employment of personnel from non-EU countries, verify the regularity of their residence permit and monitor their expiration;
- assess and regulate, with particular attention and sensitivity, the direct and/or indirect organization of trips or periods of stay in foreign places with specific regard to places known for the phenomenon of so-called "sex tourism";
- equip the Company with computer tools that prevent access to and/or receipt of material relating to child pornography;
- periodically and unequivocally remind Employees of the correct use of the IT tools in their possession.

⁷ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

H. Sensitive Processes in market abuse Offences

The main Sensitive Processes that the Company has concretely identified internally in relation to the Offences referred to in Article 25-*sexies* of the Decree are as follows:

Sensitive Processes	Predicate Offence ⁸
Management of privileged information	Article 25 <i>sexies</i> of the Decree

Specific principles of conduct

It is expressly forbidden for the persons indicated below to engage in, collaborate with or cause conduct which, taken individually or collectively, directly or indirectly constitute the types of Offences and administrative crimes considered in this section (Article 25-*sexies* of the Decree and Article 187-*quinquies* TUF). These subjects are:

- the members of the Board of Directors;
- the members of the Board of Statutory Auditors;
- the Chief Executive Officer;
- the Chief Financial Officer.

Recipients are required to:

- comply with the provisions and internal procedures concerning the management of financial and corporate communications;
- maintain a conduct based on the principles of fairness, transparency, cooperation and compliance with the laws in force both in Italy and in the countries where the Company operates, in the performance of all activities in which one comes into possession of privileged information or news that may facilitate the manipulation of information or market operations;
- refrain from carrying out simulated or otherwise fraudulent operations, as well as from spreading false or incorrect information, capable of causing a significant alteration in the price of financial instruments admitted to a regulated market;
- refrain from disseminating false or misleading market information through any means of communication.

In addition, some expressly prohibited behaviours are listed below, by way of example:

- use Privileged Information according to one's position within Stellantis Group or NHOA Group or because one has business relations with these Groups, negotiate, directly or indirectly, shares of one of the companies of the two Groups, of client or competitor companies, or of other companies to gain a personal advantage, as well as favour third parties or the Company or other companies of both Groups;
- disclose to third parties Privileged Information related to Stellantis Group or NHOA Group, except in cases where such disclosure is required by law, other regulations or specific contractual agreements with which the counterparties have committed themselves in writing to use it exclusively for the purposes for which such information is transmitted and to maintain its confidentiality;

⁸ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

- taking part in Internet forums, or chat rooms, on financial instruments or issuers of financial instruments, whether listed or unlisted, on which information is exchanged concerning Stellantis Group or NHOA Group, its companies, competitors or listed companies in general, or financial instruments issued by such entities, unless these are institutional meetings for which a legitimacy check has already been carried out by the relevant functions or there is an exchange of information whose non-privileged nature is obvious.

The Company defines the rules for establishing and maintaining a register of persons who have access to privileged information.

I. Sensitive Processes in crimes of manslaughter and serious or very serious culpable injuries (committed in breach of the regulations on health and safety in the workplace)

In the context of the Offences dealt with in this Special Section, the Reference Guidelines point out that it is impossible to exclude a priori, any sphere of activity of the Company, since the Predicate Offences, under examination, could concern all cases in which a violation of the obligations and prescriptions on health and safety at work occurs within the Company.

The Model shall provide for an appropriate control system on its implementation and on the maintenance over time of the suitability of the measures adopted.

The Company adopted an internal control system for the protection of safety in the workplace, aimed at preventing possible violations of the relevant legislation and ensuring the technical skills and powers necessary for the verification, assessment and risk management through the arrangement of a suitable organizational structure, internal rules and procedures and ongoing monitoring of processes.

This monitoring, carried out by the corporate internal functions in charge, is possibly supplemented by the activities carried out, at the request of the Supervisory Body, by external bodies and/or by the Company's Internal Audit function.

The review and possible amendment of the Model shall be adopted when significant violations of the rules on accident prevention and hygiene are discovered, or when there are changes in the organization and activity in relation to scientific and technological progress (Article 30 para. IV of Legislative Decree no. 81 of 2008).

In order to obtain formal validation of implemented measures, the Company started an activity aimed at certifying that its objectives, policies, procedures and hygiene and safety at work operating methods comply with the provisions of the UNI ISO 45001:2018 standard, thanks to the certification of its Qualified Safety Management System, by an independent third-party certifying body.

The main Sensitive Processes the Company concretely identified internally, in relation to the crimes set forth in Article 25-*septies* of the Decree are the following:

Sensitive Processes	At-Risk Activities	Predicate Offence ⁹
1. Compliance with the technical and structural standards of the law relating to equipment, facilities, workplaces and specific risks	Identification and evaluation of legal requirements, technical standards and other applicable requirements with reference to the Company's reality; Planning of controls, periodic checks and maintenance interventions; Identification of competent Company figures to purchase (in compliance with current regulations) equipment, machinery, hazardous substances and preparations.	Article 25 <i>septies</i> of the Decree
2. Risk assessment activities and preparation	Hazard identification and risk assessment (referring to all conditions applicable to the Company);	Article 25 <i>septies</i> of the Decree

⁹ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

<p>of resulting prevention and protection measures</p>	<p>Identification of implemented prevention and protection measures and personal protective equipment;</p> <p>Risk assessment review following significant changes (new activities, changes in legislation, production process or work organization, emergencies, accidents, Qualified diseases, etc.);</p> <p>Definition and implementation of the improvement plan containing the prevention and protection measures implemented, programmed according to the intervention priorities.</p>	
<p>3. Organizational activities such as emergencies, first aid, tender management, safety meetings, and worker safety representative consultation.</p>	<p>In relation to the organization of emergency and first aid situations:</p> <p>Identification of possible emergency situations and definition of actions to be taken;</p> <p>Identification and designation of persons in charge of implementing emergency management measures (fire prevention and firefighting, evacuation of workplaces, first aid, etc.);</p> <p>Drafting of the Emergency Plan, defining the organizational and management measures to be implemented;</p> <p>First-aid organization with the cooperation of the Qualified physician;</p> <p>Organization of communication arrangements with the public services responsible for emergency management (fire-fighting, first aid, etc.);</p> <p>Setting up of alarm relays;</p> <p>Layout and display of plans showing escape routes and location of fire-fighting equipment;</p> <p>Organization of annual fire and first aid drills;</p> <p>Evaluation of emergency test results, adequacy of applied management measures and possible update of the Improvement Plan.</p> <p>In relation to procurement management:</p> <p>Selection of contractors after verification of technical and professional suitability;</p> <p>Contractors' contractual duties and obligations;</p>	<p>Article 25 <i>septies</i> of the Decree</p>

	<p>Implementation of the measures envisaged by Article 26 of Legislative Decree 81/08 (obligations relating to procurement, works or supply contracts);</p> <p>Implementation of the measures provided for by Title IV of Legislative Decree 81/08 (management of temporary and mobile construction sites);</p> <p>Control of supervisors and the Compliance Officer for the work (application of the measures of Article 26 and Title IV).</p> <p>In relation to the organization of recurrent safety meetings and consultation of workers' safety representatives.</p> <p>Periodic meeting ex Article 35 D.Lgs. 81/08;</p> <p>Consultation of Workers' Representatives and powers provided for by Article 50 of Legislative Decree 81/08.</p>	
4. Health surveillance activities	<p>Verification of the qualifications and requirements of the Competent Medical Professional and implementation of health surveillance;</p> <p>Participation of the Competent Medical Professional in the risk assessment, drafting of the health protocol and definition of the frequency of health checks;</p> <p>Periodic inspection of the work environment by the Competent Medical Professional;</p> <p>Establishment and custody, by the Competent Medical Professional of workers' health records.</p>	Article 25 <i>septies</i> of the Decree
5. Information and training of workers	<p>Procedures for managing worker information and training activities;</p>	Article 25 <i>septies</i> of the Decree

	<p>Preparation and implementation of the "Annual education, information and training programme" for all Company Employees;</p> <p>Education and training for workers entrusted with the use of work equipment requiring special know-how and for that requiring special qualifications;</p> <p>Training of RSPP (Head of the Prevention and Protection Service), RLS (Workers' Safety representatives) and those in charge of emergency and first aid measures;</p> <p>Verification of the adequacy of the training delivered regarding the risks of the task to which the worker is assigned;</p> <p>Training of workers on the main aspects of the Organization and Management Model and on the roles, tasks and responsibilities of each figure involved in it;</p> <p>Collection and storage of training, information and workers' data;</p> <p>Information to workers on procedures for first aid, fire fighting and evacuation of workplaces as well as on the names of those in charge.</p>	
6. Supervisory activities with reference to compliance with procedures and instructions for safe work by workers	<p>Identification of the figures in the safety system and assignment of the relevant tasks;</p> <p>Monitoring by managers and supervisors of workers' compliance with Company regulations.</p>	Article 25 <i>septies</i> of the Decree
7. Acquisition of documentation and certifications required by law	Management and custody of compulsory certifications and all documents relating to health and safety at work.	Article 25 <i>septies</i> of the Decree
8. Periodic checks on the application and effectiveness of the procedures adopted	<p>Routine monitoring and measurement of the implementation and effectiveness of procedures adopted;</p> <p>Auditing tasks to monitor the implementation and effectiveness of applied procedures.</p>	Article 25 <i>septies</i> of the Decree
9. Systems for recording the performance of the	Definition and implementation of documentation management and safekeeping procedures	Article 25 <i>septies</i> of the Decree

tasks referred to in points 1 to 8		
10. Breakdown of functions ensuring the technical skills and powers necessary for the verification, assessment, management and control of the risk, as well as a disciplinary system capable of sanctioning non-compliance with the measures set out in the model	<p>In relation to health and safety roles and responsibilities:</p> <p>Formal definition of the internal organizational structure responsible for managing health and safety aspects in the workplace on site;</p> <p>Updating of the organization in charge of managing occupational health and safety issues in case of changes in the organizational structure of the site;</p> <p>Formal appointment of the Health and Safety Officer and of any Prevention and Protection Officers;</p> <p>Compliance with health and safety procedures and work instructions through the organizational structure in charge of supervision and control activities.</p> <p>In relation to the disciplinary system:</p> <p>Communication to all interested parties of the disciplinary and sanctioning system adopted by the Company;</p> <p>Enforcement of the disciplinary and sanction system for any behaviour in breach of the control system and/or failure to comply with obligations under occupational health and safety legislation.</p>	Article 25 <i>septies</i> of the Decree
11. Monitoring system on the fulfilment of points 1 to 10	Setting up an appropriate system for monitoring the implementation of prevention and protection measures as well as accident prevention and hygiene in the workplace.	Article 25 <i>septies</i> of the Decree

Specific principles of conduct and preventive measures

This section sets out to govern the conduct of Employers, Managers, Supervisors, Workers and Contractors.

The goal is to:

- issue a list of general principles and procedural principles, which the Recipients, to the extent to which they may be involved in the performance of Activities at Risk, are required to comply with in order to prevent the Offences of manslaughter and grievous or very grievous bodily harm, committed in breach of the rules on accident prevention and on the protection of hygiene and health at work. All this, taking into account the difference in the role of each of the subjects themselves *vis-à-vis* the Company and, therefore, the diversity of their obligations as specified in the Model;
- provide the Supervisory Body and the heads of the other corporate functions, called upon to cooperate with it in the operational tools to perform the control, monitoring and verification activities

required. In this regard, it should be noted that, given the specific nature of the subject matter, the Supervisory Body, in carrying out its activities, should necessarily avail itself of specialised personnel, not least with a view to maintaining and integrating the professionalism required for its role by the rules.

In order to allow for the implementation of the principles aimed at protecting the health and safety of workers as identified in Article 15 of Legislative Decree 81/2008 and in compliance with the provisions of Legislative Decree 81/2008 and subsequent amendments, the following is provided for.

Procedures/provisions

With regard to health and safety at work, the Company shall:

1. issue procedures/provisions aimed at formally defining tasks and responsibilities in the field of safety;
2. monitor accidents at work and regulate reporting to the National Institute for Accident Insurance (INAIL) in accordance with the law;
3. monitor occupational diseases and regulate the activity of communicating the relevant data to the National Register for Occupational Diseases set up in the INAIL database;
4. adopt an internal procedure/arrangement for organizing preventive and periodic health checks;
5. adopt an internal procedure/arrangement for the management of first aid, emergency, evacuation and fire prevention;
6. adopt procedures/provisions for the administrative management of accidents and occupational diseases.

Health and safety organizational structure

Within the Company's organizational structure, the following must be formally appointed and operate:

(i) The Employer and the Manager

The Employer is the subject holding the employment relationship with the workers or, in any case, the subject who, according to the organization type and structure within which the workers perform their activity, is responsible for the organization itself or the production unit as he exercises decision-making and spending powers. The "delegated" occupational health and safety manager (Article 16 of Legislative Decree 81/08) is the person to whom the employer's powers have been delegated, with the exclusion of the non-delegable tasks (Article 17 of Legislative Decree 81/08), *i.e.* risk assessment and preparation of the Risk Assessment Document and appointment of the RSPP (Head of the Prevention and Protection Service).

Employer and Manager have the following duties:

1. organize the prevention and protection service – the Person in charge of the Prevention and Protection Service and the Employees - and appoint the Competent Medical Professional;
2. assessing - including the use of work equipment, chemical substances or preparations, and the layout of workplaces - all the risks to the health and safety of workers, including those concerning groups of workers exposed to particular risks, including those related to work-related stress, as well as those related to differences in gender, age, nationality and the specific type of contract under which the work is carried out;

3. adapt the work to the individual, particularly as regards the design of workplaces and the choice of work equipment and methods, in particular to alleviate monotonous and repetitive work and to reduce the effects of such work on health;
4. draw up, at the end of this assessment, a document (to be kept at the Company or production unit) containing:
 - a report on the assessment of the risks to safety and health at work, specifying the criteria adopted for the assessment;
 - identification of the prevention and protection measures and of the personal protective equipment, consequent to the assessment of the first point;
 - the programme of measures considered appropriate to ensure the improvement of safety levels over time.

The assessment and drafting of the document must be carried out in cooperation with the health and safety officer, and the Competent Medical Professional, after consultation with the workers' health and safety representative, and must be repeated when there are significant changes in the production process for the purposes of the safety and health of workers, in relation to the degree of technical development or following significant accidents or when the results of health surveillance show it to be necessary. In such cases, the risk assessment document must be redrafted within 30 days of the respective causes;

5. take the necessary measures for the safety and health of workers, in particular:
 - designating in advance the workers in charge of implementing the measures for fire prevention and firefighting, evacuation of workers in case of serious and immediate danger, rescue, first aid and, in any case, emergency management;
 - updating the prevention measures in relation to organizational and production changes that are relevant to health and safety at work, or in relation to the degree of evolution of prevention and protection techniques;
 - taking into account the skills and conditions of the workers in relation to their health and safety, when assigning the relevant tasks to them;
 - providing workers with the necessary and suitable individual protection devices, in agreement with the Health and Safety Officer;
 - taking appropriate measures to ensure that only workers who have received adequate instructions enter areas which expose them to a serious and specific risk;
 - requiring compliance by individual workers with current regulations, as well as Company regulations on safety and health at work and the use of the collective means of protection and personal protective equipment made available to them;
 - sending the workers to the medical examination within the deadlines established by the health surveillance programme and requesting the Competent Medical Professional to comply with the obligations provided for by the regulations on safety at work, informing them about the processes and risks connected with the production activity;

- adopting measures to control risk situations in the event of an emergency and giving instructions so that workers, in the event of serious, immediate and unavoidable danger, leave the workplace or the dangerous area;
 - informing workers exposed to serious and immediate risks about the risks themselves and the safety specifications adopted;
 - refraining from requiring workers to return to work in a situation where serious and immediate danger persists;
 - allowing workers to verify, through the safety representative, the implementation of safety and health protection measures and allowing the safety representative to access Company information and documentation relating to risk assessment, related prevention measures, as well as those relating to dangerous substances and preparations, machinery, equipment, organization and work environments, accidents and occupational diseases;
 - taking appropriate steps to prevent the technical measures taken from causing a risk to public health or a deterioration in the outdoor environment;
 - monitoring accidents at work involving at least one day's absence from work and occupational diseases and keeping evidence of the data collected, of which the prevention and protection service and the Competent Medical Professional shall also be informed;
 - consulting the safety representative in relation to: the assessment of risks, the identification, planning, implementation and verification of prevention in the Company; the appointment of persons in charge of the prevention service, fire prevention activities, first aid, evacuation of workers; the organization of training for workers in charge of managing emergencies;
 - adopting the required measures for fire prevention and evacuation of workers, as well as for the case of serious and immediate danger. These measures must be appropriate to the nature of the activity, the size of the Company or production unit and the number of persons present;
6. agree with the Competent Medical Professional, at the time of appointment, the place of safekeeping of the health and risk records of the worker subjected to health surveillance, to be kept with safeguarding of professional secrecy; a copy of the health and risk records shall be given to the worker at the time of termination of the employment relationship, providing them with the necessary information on the preservation of the original. Each worker concerned shall be informed of the results of the health surveillance and, upon request, shall receive a copy of the health records.

(ii) The PPS Manager

They should possess professional skills and qualifications in the field of prevention and safety, namely they should:

- hold an upper secondary educational qualification;
- have participated in specific training courses appropriate to the nature of the risks present in the workplace;

- have obtained a certificate of attendance at specific training courses on risk prevention and protection;
- have attended refresher courses;

(iii) The Competent Medical Professional

They should possess one of the qualifications pursuant to Article 38 of Legislative Decree 81/2008 and, precisely:

- specializing in occupational medicine or preventive medicine for workers and psychotechnics; or
- teaching occupational medicine or preventive medicine for workers and psychotechnics or industrial toxicology or industrial hygiene or in occupational physiology and hygiene or in occupational medicine; or
- authorization referred to in Article 55 of Legislative Decree No 277 of 15 August 1991;
- specialization in hygiene and preventive medicine or in forensic medicine and proven attendance of specific university training courses or proven experience for those who, on 20 August 2009, carried out the activities of Competent Medical Professional or had carried them out for at least one year within the previous three years.

The Competent Medical Professional shall be involved in the organization of environmental monitoring and shall receive a copy of the results;

(iv) The Compliance Officer

The Compliance Officer must:

1. supervise and monitor compliance by individual workers with their legal obligations, as well as with Company regulations on health and safety at work and the use of collective means of protection and personal protection equipment made available to them and, in the event of persistent non-compliance, inform their line managers;
2. ensure that only workers who have received appropriate instructions enter areas that expose them to a serious and specific risk;
3. require compliance with the measures for controlling risk situations in the event of an emergency and give instructions so that workers, in the event of serious, immediate and unavoidable danger, leave the workplace or the dangerous area;
4. inform workers exposed to the risk of serious and immediate danger as soon as possible of the risk and of the measures taken or to be taken as regards protection;
5. refrain from requiring workers to return to the workplace in a situation where serious and immediate danger persists;
6. promptly report to the employer or to the manager both the deficiencies of work means and equipment and of the personal protective equipment, as well as any other dangerous condition occurring at work, of which they become aware based on the training received.

(v) First aiders.

These are the people designated by the Employer and adequately trained, responsible for rescue in the Company, in case of accidents.

(vi) Fire-fighters

These are the persons designated by the Employer and adequately trained, responsible for the implementation of fire-fighting and evacuation measures, in case of emergency.

(vii) Persons assigned to the Prevention and Protection Service

(viii) The Worker

The Worker must:

1. Comply with the provisions and instructions given by the employer, managers and compliance officers, for the purposes of collective and personal protection;
2. properly use machinery, equipment, tools, hazardous substances and preparations, means of transport and other work equipment, and safety devices;
3. make appropriate use of the protective equipment made available to them;
4. immediately report to the employer, the manager or the compliance officer the deficiencies of the means and devices referred to in the previous points as well as any other dangerous conditions of which they become aware, taking direct action, in case of urgency, within the scope of their competence and possibilities, to eliminate or reduce such deficiencies or dangers, informing the workers' safety representative;
5. do not remove or modify safety, signalling or control devices without authorization;
6. not to carry out on their own initiative any operation or manoeuvre that is not within their competence or that could endanger their own safety or that of other workers;
7. undergo the health checks required of them;
8. obligation to participate in the compulsory training as per Legislative Decree 81/2008 duly planned by the Company;
9. contribute, along with the employer, managers and compliance officers, to the fulfilment of all obligations imposed by the official authority or in any case necessary to protect the safety and health of workers during work.
10. persons responsible for monitoring the implementation of the maintenance/improvement measures shall be identified.

Other Company obligations

• **Information**

The Company shall:

- provide adequate information to Employees and new hires (including temporary workers, interns and *co.co.pro.* (*i.e.*, according to Italian law, project work contract)) about the Company's specific risks, their consequences and the prevention and protection measures taken;
- give evidence of the information provided for the management of first aid, emergency, evacuation and fire prevention and any meetings must be recorded;

- inform the Employees and new hires (including temporary workers, interns and co.co.pro.) about the appointment of the PPS Manager, the qualified physician and the persons in charge of the specific tasks for first aid, rescue, evacuation and fire prevention;
- formally document the information and instruction for the use of the work equipment made available to the Employees;
- involve the PPS Manager and/or the Competent Medical Professional in the definition of information programmes;
- organize regular meetings between the relevant occupational safety functions;
- involve the Workers' Safety Representative in the organization of risk detection and assessment activities, in the appointment of fire prevention, first aid and evacuation personnel.

- **Training**

The Company shall:

- provide adequate training to all Employees in the field of safety at work;
- have the PPS Manager and/or the Competent Medical Professional participate in the drafting of the training plan;
- provide evaluation questionnaires in relation to the training delivered;
- adapt the training to suit the risks of the task which the worker is actually assigned to;
- prepare a specific training plan for workers exposed to serious and immediate risks;
- provide preventive, additional and job-specific training for workers who change jobs and those who are transferred;
- provide, through the Employer, adequate and specific training and periodic updates for managers and compliance officers, in relation to their duties in the field of health and safety at work;
- provide specific training for persons in charge of specific prevention and protection tasks (fire prevention, evacuation, first aid);
- carry out periodic evacuation drills of which evidence must be provided (minutes of the drill with reference to participants, progress and results).

- **Registers and other documents**

The Company is required to comply with the following requirements:

- the accident register must be kept up to date and be fully complete;
- in the event of exposure to carcinogens or mutagens, a register of exposed persons must be prepared;
- documentary evidence must be provided of the visits to the workplace carried out jointly by the PPS Manager and the Competent Medical Professional;
- the Company must keep a file relating to compliance with safety and hygiene at work requirements;
- the risk assessment document (DVR) may also be kept in electronic form and must be dated or certified by the employer's signature, as well as, for the sole purpose of proving the date, by the signature of the PPS Manager, the WHSR or workers' representative for territorial safety and the Competent Medical Professional;

- the risk assessment document (DVR) must indicate the criteria, tools, and methods used to assess risks. The choice of criteria for drafting the document is the responsibility of the Employer, who shall provide for it according to criteria of simplicity, brevity and comprehensibility, so as to guarantee its completeness and suitability as an operational tool for planning Company interventions and prevention;
- the DVR must contain the programme of maintenance and improvement measures.

- **Meetings**

The Company must organize regular meetings between the functions in charge, in which the Supervisory Body may participate, by formally convening meetings and taking minutes of them signed by the participants.

- **Procurement contracts**

In the context of the conclusion and execution of procurement contracts, the Company is bound by the following obligations.

(i) Relations with contractors

The Company must prepare and keep updated the list of companies operating on its sites under contract.

The methods for managing and coordinating contracted work must be formalized in written contracts in which there are express references to the obligations set forth in Article 26 of Legislative Decree 81/2008, including the obligations of the Employer to:

- verify the technical-professional suitability of the contractors in relation to the work to be contracted out, also by means of registration with the Chamber of Commerce, Industry and Crafts;
- provide detailed information to contractors on the specific risks existing in the environment in which they are to operate and on the prevention and emergency measures adopted in relation to their activities;
- cooperate in the implementation of the measures of prevention and protection from the risks at work incident to the work activity that is the subject of the contract and coordinate the measures of protection and prevention from the risks to which the workers are exposed;
- adopt measures aimed at eliminating risks due to interference between the work of the various companies involved in the execution of the overall work.

Except in the case of intellectual services, mere supplies of materials or equipment, as well as works or services whose duration does not exceed five person-days, (person-days means the presumed value of the works, services and supplies as the sum of the number of person-days necessary to carry out the works, services and supplies. This value shall be considered with reference to the time span of one year from the beginning of the works) - if they do not involve risks indicated in Article 26 paragraph 3-*bis* of Legislative Decree 81/08 - the Employer shall arrange/organize a joint risk assessment with the contracting companies. The commissioning employer and the contractor must draw up a single risk assessment document (DUVRI) detailing the measures taken to eliminate any interference. This document must be attached to the procurement or work contract and must be adapted according to the progress of the works, services and supplies.

Contracts of employment, procurement and subcontracting must clearly state the costs related to work safety (which are not subject to discount). The workers' representative and trade unions can access these data, on request.

The management of occupational safety obligations in the case of subcontracting must be clearly defined in the procurement contracts.

The employer is jointly and severally liable with the contractor, as well as with each of the subcontractors, for all damages for which the worker, employed by the contractor or the subcontractor, is not indemnified by the National Institute for Insurance against Accidents at Work.

In the context of contracting and subcontracting activities, the personnel employed by the contractor or subcontractor must be provided with an identification card with a photograph containing the personal details of the worker and the Employer.

(ii) Relations with contractors

The Company must prepare and keep up-to-date a list of the companies in which it operates as a contractor.

The Company must request information from the companies where it operates as a contractor about the specific risks and the preventive measures they adopted.

If the work is subcontracted, procedures for managing and coordinating the subcontracted work must be defined.

The cost of safety at work must be specifically mentioned in procurement/works contracts.

- **Suppliers' obligations**

Suppliers shall comply with the prohibition to manufacture, sell, rent and lease work equipment, personal protective equipment and installations, which do not comply with the laws and regulations in force on health and safety at work.

In the case of financial leasing of goods subject to conformity certification procedures, the latter must be accompanied by the relevant documentation by the lessor.

- **Purchase of equipment, machinery and installations**

The purchase of equipment, machinery and installations must take place after evaluation of their safety requirements and in compliance with the applicable regulations in force (e.g. EC marking, declaration of conformity issued by the installer, etc.).

Where required by the standards in force, their commissioning will be subject to verification and testing procedures.

Workers in charge of the use of new equipment, machinery and installations must be adequately trained.

Disciplinary system

Further to what stated in Section IV of the Model, please note that failure to comply with measures and principles of conduct to protect the health and safety of workers constitutes a disciplinary Offence punishable under the terms of the CCNL Metalworkers/Journalists.

J. Sensitive Processes in crimes of receiving of stolen goods, money laundering and utilization of money, goods or benefits of unlawful origin, and self-laundering.

The main Sensitive Processes that the Company concretely identified internally in relation to the Offences referred to in Article 25-*octies* of the Decree are as follows:

Sensitive Processes	At-Risk Activities	Predicate Offence ¹⁰
Management of financial flows	Management of relations with suppliers/customers/Partners Management of receivable/payable accounts and general accounting Management of investments and extraordinary transactions Management of fiscal/tax obligations Management of intercompany transactions and transfer pricing Current accounts management	Article 25 <i>octies</i> of the Decree

Specific principles of conduct

In addition to what is set out in the paragraph "**General Control Environment**", at the beginning of this section, a number of additional principles of conduct are listed below, which must be observed specifically for the effective prevention of the risk of committing Offences of receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin as well as self-laundering. Furthermore, these behavioural principles constitute a protection aimed at guaranteeing the correctness of the elements that determine the tax returns as well as preventing the Predicate Offences provided for by Article 25- *quinquies decies*:

- request the necessary information in order to assess the reliability, economic soundness and commercial/professional reliability of suppliers and Partners;
- behave correctly, transparently, in good faith and collaboratively, in compliance with the law and internal Company procedures, in all activities aimed at managing supplier and customer records;
- determine the minimum requirements to be met by tenderers and setting the criteria for evaluating tenders in standard contracts;
- identify a function responsible for defining technical specifications and evaluating bids in standard contracts;
- identify a body/unit responsible for the execution of the contract, indicating tasks, roles and responsibilities;
- determine the criteria for selecting, entering into and executing agreements/joint ventures with other companies for the implementation of investments;

¹⁰ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

- ensure transparency and traceability of agreements/joint ventures with other companies for the implementation of investments;
- verify the economic adequacy of any investments made in joint ventures (compliance with average market prices, use of trusted professionals for due diligence operations);
- in relation to extraordinary transactions, involve the fiscal office for the economic assessments underlying such transactions;
- promptly and correctly record operations/transactions in accordance with the criteria provided for by law and based on the applicable accounting principles;
- verify the completeness of the documentation relating to the management of receivable/payable accounts;
- check that the Company providing the service is the same one issuing the invoice;
- verify that any payments to be processed manually comply with the controls provided for by Company procedures and the authorization levels defined;
- verify the regularity of the payments/collections, with reference to the full coincidence between the recipients/orderers of the payments and the counterparties actually involved in the transactions;
- carry out formal and substantial controls of corporate cash flows, with reference to payments to third parties and payments/transactions with companies of the Stellantis Group or the NHOA Group;
- verify that the provision of goods and/or services, in the context of relations with companies of the Stellantis Group or the NHOA Group, are in line with market values and are adequately contracted;
- verify and periodically update the list of persons formally delegated and authorised to operate on the Company's bank accounts;
- verify that bank accounts are properly reconciled;
- provide adequate training and information programmes for all Employees working in the Company departments involved in the preparation of the financial statements and other related documents, as well as in the Company departments that deal with tax compliance;
- check that investment initiatives comply with the authorization levels and rules defined in Company policies;
- refrain from having business relations with persons (physical or juridical) who are known or suspected to belong to criminal organizations or in any case operating outside the law, such as, for example, persons linked to money laundering, terrorism, drug trafficking, usury, etc.;
- refrain from contracting or, in general, having business contacts with natural persons and legal entities residing or having their headquarters in a country included in the lists of countries considered as non-cooperative by the Financial Action Task Force on Money Laundering (hereinafter "FATF" - www.fatf-gafi.org);
- refrain from having contacts with individuals on the anti-terrorism blacklist available on the site <http://www.consilium.europa.eu/it/policies/fight-against-terrorism/terrorist-list>;
- pay particular attention to payments received from foreign credit institutions/customers.

In preparing tax returns relating to income tax, indirect taxes and other local taxes, the Company shall:

- verify the effective correspondence between the indicated receivables/payables and the existing ones by using the invoices related to the operations carried out as well as the amounts contained in the accounting records;
- comply strictly with the deadlines laid down by the applicable legislation for submitting them and for the subsequent payment of taxes.

It is also necessary to:

- refrain from accepting payments in cash, beyond the legal limits in force;
- refrain from purchasing goods or services at a price that is clearly lower than the market value, without first checking their origin;
- in the case of handling payments/collections through a cash-filled petty cash, formally identify the petty cash manager and have a procedure in place to regulate its proper use;
- refrain from using anonymous instruments to carry out transfer operations of significant amounts;
- refrain from issuing bank or postal cheques for amounts greater than those provided for by current regulations that do not bear the indication of the name or company, name of the beneficiary and the non-transferability clause;
- refrain from endorsing for collection bank and postal cheques issued to the order of the drawer to parties other than banks or Poste Italiane S.P.A.;
- refrain from making deposits into numbered current accounts or at credit institutions without physical locations;
- refrain from making monetary donations to individuals, companies or organizations convicted of illegal activities;
- refrain from carrying out any operation aimed at creating non-accounting funds;
- refrain from transferring money and bearer securities (cheques, postal orders, certificates of deposit, etc.) for amounts exceeding the limits of the law in force, except through authorized intermediaries, such as banks, electronic money institutions and Poste Italiane S.P.A.;
- keep evidence, in special records on computer files, of transactions carried out on current accounts opened in countries that provide for more lenient transparency rules and managed independently for overall amounts exceeding the legal limits in force.

K. Sensitive Processes in Offences related to copyright infringement

The main Sensitive Processes that the Company identified internally in relation to the Offences referred to in Article 25-*novies* of the Decree are as follows:

Sensitive Processes	At-Risk Activities	Predicate Offence ¹¹
Installation, maintenance, updating of <i>software</i> provided by third parties	Performance by the Company of activities of duplication of computer <i>software</i>	Article 25- <i>novies</i> of the Decree
	Reproduction, transfer to another medium, distribution, communication of the contents of a database	
Use of computer/telematics systems to support work activities	Reception/dissemination of a protected intellectual work	Article 25- <i>novies</i> of the Decree
	Entry into computer network systems for the purpose of promoting the brand/product of a third party's intellectual work	
Development, implementation and coordination of advertising and promotional initiatives	Organization of promotional events	Article 25- <i>novies</i> of the Decree
	Sponsorships	
	Preparation of advertising projects/products	
	Management of relationships with specialized agencies for the organization of events and/or development of advertising products	
	Selection of commercial Partners and formalization of commercial relations	

The risk of committing the Offences referred to in this Section may materialise to a greater extent in certain areas (activities, functions, processes), among which the sectors where staff work in the promotion of Company products, development of advertising products, management of Company software, are of central importance, given the specific skills and know-how of Employees working in this area.

Specific principles of conduct

In order to protect the above-mentioned Sensitive Processes, reference is made to the principles laid down on the subject of computer-related crime. In particular, it is appropriate to:

- inform users of computer systems that the software assigned to them is protected by copyright laws and as such is prohibited from being duplicated, distributed, sold or held for commercial/entrepreneurial purposes;
- adopt corporate rules of conduct that concern all Company personnel as well as third parties acting on behalf of the Company;

¹¹ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

- provide the Recipients with adequate information regarding the works protected by copyright and the risk of committing this Offence.

In addition to what reported in the paragraph "**General Control Environment**", at the beginning of this section, some additional principles of conduct are listed below, which must be specifically observed for an effective prevention of the risk of committing Offences related to violation of copyright:

- protect the copyright on data, images and/or software developed by the Company and of strategic value for the same through: industrial secret, when and where legally possible and/or (for Italy) SIAE registrations;
- use disclaimers on presentations, technical documentation, commercial documentation that clearly identify the copyright holder and the date of creation;
- prohibit the employment/use/installation of copied/unmarked/unauthorised material on the IT tools provided by the Company;
- prohibit the downloading of copyrighted software;
- in the context of the promotion/publication of brands/products and, in particular, in the management of events, the use, availability to the public also through a system of telematic networks, of protected intellectual works, must take place in compliance with the regulations on copyright;
- allow the use of parts of works, as well as the quotation or reproduction of other people's works on condition that they are not traded or, in any case, that they do not constitute competition for the economic use of the work itself;
- allow free of charge publication through the Internet of low-resolution or degraded images/music for educational or scientific use only, or otherwise non-profit making;
- provide, in contractual relationships with Partners/third parties, for indemnity clauses aimed at holding the Company harmless from any liability in the event of conduct, carried out by the same, which may result in the violation of any copyright;
- include clauses that relieve the Company from any prejudicial consequences deriving from third party claims regarding the alleged violation of copyright.

By way of example, it is also prohibited to:

- counterfeit or alter trademarks or distinctive signs, national or foreign, of industrial products, being aware of the existence of the industrial property title or make use of counterfeited or altered trademarks or distinctive signs;
- counterfeit or alter industrial patents, designs or models, domestic or foreign, or make use of such counterfeit or altered patents, designs or models;
- introduce into the territory of the State, in order to make a profit, industrial products with counterfeit or altered trademarks or other distinctive signs, national or foreign;
- hold for sale, put on sale or otherwise put into circulation, in order to make a profit, industrial products marked with counterfeit or altered trademarks that could induce the purchaser to exchange them with other known ones, creating possible confusion among customers and such as cause significant damage to the owner of the counterfeit trademark;

- deliver to the purchaser a movable item for another, or a movable item, by origin, source, quality or quantity, different from that stated or agreed;
- sell or otherwise put into circulation intellectual property or industrial products, with names, trademarks or distinctive national or foreign signs, designed to mislead the buyer about the origin, source or quality of the work or product;
- industrially use objects or other goods made by usurping an industrial property right or in violation of the same, being aware of the existence of the industrial property right;
- introduce into the territory of the State, hold for sale, put on sale with a direct offer to consumers or otherwise put into circulation objects or other goods made by usurping an industrial property right or in violation of the same, in order to make a profit.

L. Sensitive Processes in environmental crimes

Safeguarding the environment is a key element in the management of the Company's business, and the Company is committed to continually improving its environmental performance, evaluating all investment opportunities that may be necessary to achieve this.

The Company, with the aim of formally validating what has already been implemented, started an activity at its national plants to certify that its objectives, policies, procedures and operating methods are compliant with the standards set out in UNI-EN ISO 14001:2011 and obtained the relative certificate of conformity from a third-party, independent certification body.

Uniformity in organization and standardized processes and environmental management systems is required for the effective achievement of environmental objectives.

The main Sensitive Processes that the Company concretely identified internally are the following:

Sensitive Processes	At-Risk Activities	Predicate Offence¹²
Waste management	Classification of waste generated Collection and deposit of waste in the plant Waste recovery and disposal directly or through third parties Waste disposal either directly or via third parties	Article 25- <i>undecies</i> of the Decree
Ozone depleting substances		Article 25- <i>undecies</i> of the Decree
Management of relationships with suppliers/Consultants/Partners	Qualification and selection of suppliers/Consultants/Partners Contractual relations	Article 25- <i>undecies</i> of the Decree

Specific organizational principles

In addition to what reported in the paragraph "**General Control Environment**", some additional principles of conduct are listed below, which must be specifically observed for an effective prevention of the risk of committing the Offences in question.

These principles, mostly contained in the Environmental Management System adopted by the Company, are aimed at ensuring compliance with environmental regulations and the provisions contained in the Decree and at preventing events that may generate forms of pollution, minimizing the impact of production processes on the environment.

Furthermore, the Environmental Management System is aimed at preventing possible violations of the legislation and at ensuring the technical skills and powers necessary for the verification, assessment and

¹² For a detailed description of the individual cases and the relevant sentencing, see Annex A.

management of risk through the provision of a suitable organizational structure, internal rules and procedures.

Processes are constantly monitored by the Company's internal departments in charge, and may be supplemented by the activities carried out, at the request of the Supervisory Body, by external bodies and/or the Internal Audit department.

Production unit organization and allocation of responsibilities

An internal operational structure in charge of the Environmental Management System must be set up (e.g. persons in charge of specific environmental management tasks, organization charts, job descriptions, etc.). If suppliers or Partners are permanently present in the production unit, a brief description of their activities/tasks must also be provided.

The Company shall also appoint one or more Management Representative(s) for the Environmental Management System (EMS), by means of a specific appointment, giving him/her the role, responsibility and authority to

- ensure that the EMS is established, implemented and maintained in accordance with the requirements of ISO 14001:2011, the legal requirements and other requirements voluntarily signed by the organization;
- report, periodically, to the Management of the production unit on the progress of the EMS for the purposes of review and continuous improvement.

Environmental Policy: development and circulation

The Management shall issue the Environmental Policy, which is a statement of principle that establishes the Company's commitment to environmental protection, compliance with current legislation on the subject, the provisions voluntarily signed and the continuous improvement of its management system.

The Management shall ensure that the Policy is appropriate to the nature, scale, and environmental impacts of its operations, products, and services and that it is regularly reviewed and updated.

The Environmental Policy shall be distributed within the Company, as well as to suppliers and contractors present on the site. The Environmental Policy is also made available to anyone (stakeholders, customers and the general public) who requests it.

Environmental aspects

Using a specific procedure, the Company shall identify and assess the environmental aspects associated with its operations, products or services in ordinary and extraordinary conditions, also taking into account the activities carried out by personnel belonging to third party companies.

Findings shall be analysed at management review meetings and used as a basis for reviewing the principles of environmental policy, objectives and programmes.

Identification, access and evaluation of regulatory requirements

The Company shall identify the legal and other requirements it has signed up to in the environmental field.

The requirements shall be analysed for applicability within the production unit and distributed as appropriate.

It is also necessary to ensure periodic monitoring and evaluation of compliance with the requirements applicable to the production unit.

Main documents and records

The Company must make available and keep up-to-date the following documentation:

- Environmental Management Manual;
- Environment Policy, objectives and targets;
- General Procedures, Operating Procedures and Work Instructions;
- registrations, including permits, required by ISO 14001;
- documents necessary to ensure the planning, operation and control of processes relating to significant environmental aspects (e.g. loading/unloading registers, waste identification forms, maintenance activity registers, etc.).

Information and training

The Company shall provide adequate information and training to Employees and new hires (including temporary workers, interns and co.co.pro) in relation to:

1. the importance of aligning one' s behaviour with the Environment Policy, the adopted procedures and the EMS requirements;
2. the significant environmental aspects and impacts associated with their work, as well as the benefits of improved individual performance.

In order to ensure that all relevant staff have received adequate training, an annual training plan should be drawn up, including, where possible, assessment questionnaires/specific learning tests.

Workers who change tasks and those who are transferred shall receive preventive, additional and specific training for the new task.

Operational control, monitoring and measurement

Environmental operating criteria defined by the Company in its Operating Procedures and Work Instructions shall be distributed to suppliers, Consultants and Partners if their activities are related to environmental aspects.

The Company is also required to monitor and measure performances that have a significant impact on the environment.

Internal Audits and Management Review

The Company shall develop a procedure for planning, carrying out and recording internal audits on the EMS, setting out the basic principles, criteria and methods for their implementation, as well as providing guidelines for the selection and training of auditors.

The effectiveness and efficiency of the EMS is assessed as part of the Management Review, during which management becomes aware of the need for continuous improvement of the system in order to minimise its environmental impacts.

Specific principles of conduct and preventive measures

Waste management

Waste management shall be carried out in accordance with the precautionary and preventive principles, involving all actors who can have an impact on the quality and quantity of the waste generated and, if necessary, drawing on the advice of specialised third parties.

The Company shall:

- identify one or more internal functions responsible for the correct management of waste that will interface with the external bodies in charge of waste transport and disposal activities;
- to guarantee the correct administrative and legal management of waste, from the place of generation to final disposal, and to be able to certify the implementation of the necessary fulfilments to the public bodies in charge of controls;
- pursue the objective of reducing the quantity and hazardousness of waste produced;
- promote the separate collection and correct separation of waste - essential to increase its reuse/recovery and favour recovery over disposal;
- ensure the proper separation of waste by providing specific procedures to avoid the mixing of hazardous waste and hazardous waste with non-hazardous waste;
- refrain from using, even occasionally, the Company or one of its organizational units for the purpose of enabling or facilitating the commission of the Offences at issue;
- monitor the Company procedures that have a direct or indirect relevance in terms of recovery and/or disposal of waste in order to periodically assess the appropriateness of updates due to anomalies found in the related activity;
- make Company representatives aware of the degree of risk involved in their activities.

Furthermore, the Company, taking into account its own organization and the legal requirements applicable also at local level, must define, through a specific procedure, the control methods to adopt in the management of waste with particular attention to the following activities:

- **classification of waste produced:**
 - identify the activities or processes that generate waste and determine for each waste the information regarding chemical, physical, qualitative and quantitative characteristics, the activity and/or the plant of origin;
 - carry out the classification according to the descriptions and codes of the European Waste Catalogue (EWC) provided for by the regulations in force on the subject and through chemical and process analysis, possibly using the advice of third parties;
 - identify the different possibilities of waste destination (recovery, treatment, waste-to-energy, incineration, landfill);
 - periodically repeat the waste characterization analyses and, in any case, whenever new types of waste are produced;
 - take into account any change in direct materials, auxiliary materials and any change in the process, which may result in the generation of a new waste or the variation of existing ones;
- **management and control of authorizations:**

- Identify the person who, on the occasion of each waste delivery operation to third party transporters and disposers, checks:
 - the existence and validity of the authorization of the supplier performing the transport;
 - registration in the National Register of companies that carry out waste management for the type of transport of that waste;
 - the validity of the authorization of the recipient/disposer of the waste;
 - that the number plate of the vehicle that will transport the waste is indicated in the authorization/registration in the National Register;
 - that the quantity of the load does not exceed the maximum capacity of the vehicle;
 - that the purchasing Company has sent the prescribed communication of commencement of activity for carrying out recovery operations for that type of waste, in the case of waste destined for recovery;
 - guarantees from disposers and transporters;
- for the transport of dangerous goods/waste (subject to ADR regulations), ensure the presence of the specific figure of the "ADR consultant", both in the case in which the activity is carried out directly by the Company using its own personnel, and in the case of subcontracting to external suppliers;
- **management of waste accompanying documents and communications to public bodies:**
 - entrust to appropriately trained personnel the compilation and verification of administrative documentation relating to waste management and in particular the loading and unloading registers, waste identification forms (FIR) and the Single Annual Waste Declaration Form (MUD);
 - have a system to verify the return of the fourth copy of the FIR within the time limits established by the standard;
 - identify the person responsible for communicating data to public bodies, where required by the local regulations in force (e.g. sending the MUD, fill out the waste section for the E PRTR - European Pollution Release and Transfer Register - declaration, ADR annual report);
- **management of temporary waste storage/waste separation area:** entrust management to appointed personnel who will:
 - verify that each waste is deposited in the established and properly identified areas;
 - check the quantities present in order to guarantee the correct compilation of the loading and unloading operations on the register and guarantee supervision during opening hours;
 - organize disposal activities so that the time and management conditions required by current legislation are met;
- **definition of surveillance checks:**
 - provide controls on incoming supplier authorizations;
 - participating in the weighing of incoming and outgoing vehicles;

- carry out sample checks on outgoing vehicles to verify that the material loaded corresponds to that indicated in the sales order and/or in the transport documents and in the FIR.

Use of ozone depleting substances

The Company that produces and/or uses cooling, conditioning and air-conditioning equipment, containing ozone layer depleting substances (ODS), must manage these substances through procedures that allow for the types covered:

- to comply with the marketing ban also by paying attention to the divestment and disposal of plants;
- to respect retention times also with reference to the prohibition of topping up during, for example, maintenance activities.

Management of relationships with suppliers/Consultants/Partners

The Company relies on suppliers/Consultants/Partners to carry out certain activities, including the transport, disposal, recovery and sale of waste.

The selection of Consultants/suppliers/Partners and mutual relations must be based on the following principles:

- selection should be carried out in full compliance with the Company's procedures, in such a way as to be able to constantly assess the existence of the technical and legal requirements for the exercise of the activity entrusted to them, avoiding, moreover, that selection is based exclusively on economic reasons (so as to avoid the recourse to poorly qualified companies that work below cost by using illegal methods);
- favour Consultants/suppliers/Partners with UNI EN ISO 14001:2011 certified or EMAS registered Environmental Management Systems;
- verify their commercial and professional reliability by collecting, by way of example but not limited to, the following documents:
 - registration with the Chamber of Commerce;
 - self-certification as per Presidential Decree 445/00 on pending charges or sentences passed against them;
 - copy of the registration certificate in the National Register of Environmental Managers;
 - authorization by facilities of final destination of waste;
 - waste transport permits;
- contracts with Consultants/Suppliers/Partners should include clauses:
 - by which they undertake to respect and ensure that their Employees, third party auxiliaries and any sub-contractors respect the rules of law for the protection of the environment;
 - by which they declare and guarantee that they are in possession of all the administrative authorizations necessary for the performance of the services covered by the contract;
 - enabling the Company or its authorised agents to carry out inspections, checks and controls on activities related to key environmental aspects;
- provide information and training meetings with the Consultants/suppliers/Partners operating in the plant, on awareness of the Environmental Policy, key environmental aspects and their management methods;

- as a preventive measure and in the course of the relationship, check the authorizations of suppliers/contractors to whom the transport activity is assigned (as contractors or subcontractors) and of the destination sites, both for disposal and recovery operations.

M. Sensitive Processes in tax crimes

The main Sensitive Processes that the Company concretely identified internally in relation to the Offences referred to in Article 25- *quinquiesdecies* of the Decree are as follows:

Sensitive Processes	Predicate Offence ¹³
Management of invoicing, accounting data and drafting of income or value-added tax declarations for the calculation of taxes payable	Article 25 <i>quinquiesdecies</i> of the Decree
Management of the issue or release of invoices payable or other accounting documents	
Applied withholding taxes	
Management of intra-Community transactions	

General principles of conduct

In addition to what stated in the paragraph, "**General control environment**" at the beginning of this section, and to the specific principles of conduct indicated in paragraph 2.10 (Offences of receiving stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering), some general principles of conduct are listed below, which shall be observed in a specific way for effective prevention of the risk of committing tax crimes.

It is forbidden to:

- engage in conduct such as to constitute the types of Offences provided for in Article 25- *quinquiesdecies* of the Decree, concerning the tax crimes shown in Annex A;
- represent or transmit for processing and representation in annual income returns or VAT declarations, false, incomplete or, in any case, untrue data, or prepare invoices or other documents for fictitious transactions;
- issue invoices or other documents for fictitious transactions;
- omit to communicate data and information required by the regulations and procedures in force concerning the economic and financial situation of the Company;
- using invoices or other documents for fictitious transactions to evade income tax or value added tax;
- behave in such a way as to prevent, through the concealment of documents or the use of other fraudulent means, or obstruct the performance of control and audit activities by shareholders and the Board of Statutory Auditors;
- perform services or make payments to collaborators, suppliers, Consultants, or other third parties who work on behalf of the Company, which are not adequately justified in the context of the contractual relationship established with them or in relation to the type of task to be performed and current local practices;

¹³ For a detailed description of the individual cases and the relevant sentencing, see Annex A.

- provide the tax authorities with untrue documentation, conceal important information and, more generally, obstruct their control activities;
- carry out objectively or subjectively simulated transactions or use false documents or other fraudulent documents to obstruct the assessment of the financial administration and evade income tax or value added tax.

In general, it is required to:

- comply with all the provisions of the law protecting the integrity and effectiveness of the Company's assets in order not to damage the guarantees of creditors and third parties in general;
- ensure the regular functioning of the Company and of the Corporate Bodies, guaranteeing and facilitating all forms of internal control over the management of the Company provided for by law and by the Articles of Association;
- draw up and keep constantly updated a calendar, including an informative one, highlighting the obligations required for sending income tax and VAT returns;
- ensure the completeness, truthfulness and transparency of data and documentation transmitted;
- check operations and their correspondence with reality in order to avoid objective simulations;
- verify the subjects involved in order to avoid the emergence of subjective simulations (interposed subjects);
- ensure that all documentation and correspondence with the Public Administration is filed in the area designated for this purpose, broken down by history and type of taxes declared/paid.
- keep accounting records and other documents that must be kept for tax purposes in a correct and orderly manner, preparing physical and/or computerised defences that prevent any acts of destruction and/or concealment.
- verify the existence and operation of business Partners (e.g. suppliers, Consultants, distributors, dealers and customers).
- carry out with the utmost diligence and professionalism the fulfilments towards the Financial Administration and, more in general, towards third parties, so as to provide clear, accurate, complete, faithful and true information, avoiding and in any case reporting, in the appropriate form and manner, any situations that could lead to the occurrence of the Predicate Offences.
- check and monitor periodically, before carrying out intra-Community operations, that the third parties (suppliers, exporters, dealers, customers, etc.) with which the Company has commercial relations are registered in the VIES (*VAT information exchange system*) archive.
- carry out specific checks in the event of non-registration of the trading Partner in VIES.
- implement procedures for the management of financial resources in compliance with the principles of transparency and traceability set out in this Model.
- ensure that accounting records are properly maintained.
- guarantee the correct management of tax policy, also with regard to any transactions with countries on the so-called "*black list*" defined in the regulations in force and with those with a privileged tax regime indicated in the Ministerial Decree of 23 January 2002 and subsequent amendments and additions.

- identify and implement specific internal audit programmes with particular regard to the management of payments and treasury, agreements/joint ventures with other companies, intercompany relations, as well as relations with counterparties with registered offices and/or operations in countries with privileged taxation.
- provide continuous training and information for Company representatives on issues relating to the prevention of tax evasion.

Specific principles of conduct

Below is a list of some further specific principles of conduct that must be observed in order to effectively prevent the risk of committing tax crimes.

When preparing annual income tax and value added tax returns, the Company shall ensure that Company Representatives - within the scope of their respective competences:

- do not declare fictitious liabilities by means of invoices or other documents of similar evidential value to invoices, for non-existent transactions;
- do not indicate assets for an amount lower than the actual one or fictitious liabilities (e.g. fictitious costs incurred and/or revenues indicated in an amount lower than the actual one) leveraging on a false representation in the compulsory accounting records and using suitable means to hinder the assessment;
- do not show a tax base lower than the actual tax base by showing assets for an amount lower than the actual one or fictitious liabilities;
- do not unnecessarily delay the deadlines laid down by the applicable legislation for submitting them and for the subsequent payment of the resulting taxes..

In the management and monitoring of financial flows:

- The Company uses or employs only economic and financial resources whose origin has been verified and only for operations that have an express reason and that are recorded and documented.
- The management of orders and invoices is the responsibility of the AFC function through internal management systems that guarantee the traceability of operations.
- Payments are only made against duly registered invoices linked to duly filed purchase orders.
- All payments and financial flows must be properly substantiated and regularly recorded in the Company's management system so that they can be tracked and reconstructed on an *ex post* basis.
- It is essential that agreements, purchase orders, invoices and payments, including those relating to the amounts to be paid to the tax authorities and social security bodies, are checked for correspondence, with close attention paid to the authorizations signed by the persons delegated to this task;
- It is essential that payments made to collaborators and members of the Corporate Bodies correspond to the actual activity carried out, which must necessarily be accompanied by appropriate evidence;

- Payments may not be ordered/accepted from persons holding current accounts registered in tax havens and/or countries belonging to the so-called "Black List" and "Grey List", unless it is in the country in which they reside or in which the service has been performed;
- No payment may be made in cash, for eligible petty cash expenses;

When the Company acts as a supplier to a habitual exporter and receives a declaration of intent from the customer, it should:

- check electronically (on the Inland Revenue website) that the usual exporter has submitted the declaration of intent;
- issue an invoice for a non-taxable transaction for VAT purposes.

When the Company issues statements of intent to its suppliers, it should:

- check its available ceiling;
- submit a declaration of intent to the Inland Revenue Agency;
- check the degree of use of the declaration of intent against invoices received without VAT being charged.

When the Company is acting as a tax-withholding agent, it must:

- collect the relevant documentation required by law in order to correctly apply the withholdings foreseen for the various types of payments;
- keep such documentation and make it available for internal control and audit purposes.

When the Italian Company holds, directly or indirectly, including through trust companies or third parties, control of a non-resident company, it should:

- verify, also with the help of suitable IT tools, the existence of the conditions that determine whether or not the regulations on Foreign Subsidiaries are applicable.

When the Company is involved as a participant, promoter or informed party in aggressive planning transactions under DAC 6, it should:

- notify the relevant Inland Revenue Agency of the details of the transaction in question, after an analysis of the case, which can also be carried out using specially developed IT tools.