ORGANIZATION, MANAGEMENT AND CONTROL MODEL

PURSUANT TO LEGISLATIVE DECREE 231/2001

Approved by the Board of Directors on October 22nd 2007,

and last updated on September 26th 2022

FATA S.p.A. (with sole shareholder) - Management and coordination by Danieli & C. - Officine Meccaniche S.p.A.
Registered offices: Strada Statale n. 24 Km 12 - 10044 Pianezza (Torino) - Italy - PEC fata-main@pec.fatagroup.it - tel. +39 011 9668.1 - fax +39 011 9672673 - Cap. Soc. € 5.000.000 i.v. - R.E.A. Torino 1022875 - Reg. Imprese di Torino e Cod. Fisc. - P.IVA 09080800015 - www.fatagroup.it

FATA
Part of Danieli Group

TABLE OF CONTENTS

ATTACHMENTS

1. CODE OF ETHICS
2. LIST OF PREDICATE OFFENCES
3. ORGANIZATIONAL STRUCTURE
4. EVIDENCE SHEETS
5. FLOWS AND THRESHOLDS

GENERAL SECTION

FOREWORD

FATA S.p.A., a Joint Stock Company with a sole shareholder (hereinafter "**FATA**" or "**Company**"), under a more wide-ranging company policy that is sensitive to the need to ensure conditions of fairness and transparency in the running of its corporate affairs and business, in order to safeguard the Company and its shareholders, has decided to analyze and strengthen all of the corporate control and *governance* mechanisms that have already been adopted, by implementing and regularly updating the Organization, Management and Control Model (hereinafter "**Model**"), pursuant to Legislative Decree n. 231/2001 (hereinafter "**Decree**"), which is lean and flexible since it is intended for a "small company", as per the directives set forth in the Confindustria guidelines, according to which:

" … A small company, the definition of which is to be found in the essential nature of the internal hierarchical and operational organization, rather than in quantative parameters..."

The fundamental activities carried out to comply with the requirements of the Decree are:

Identifying Risks

Analysis of the company environment to determine which areas and sectors are at risk of predicate offences being committed, as well as the types of conduct that are warning signs that a predicate offence could be committed.

Planning a Protocol System

Evaluation and possible revision of the Company's existing control system, in terms of its ability to effectively counteract - i.e. reduce to an acceptable level - the identified risks.

Code of Ethics and Disciplinary System

Adoption of the controlling company's Code of Ethics, adapted to suit the specific situation of the company (ATT. 1).

Supervisory Committee

Appointment of the company's own Supervisory Committee

1. LEGISLATIVE DECREE 231/2001

The Decree - partially implemented by Delegated Law 300 dated September 29, 2002, and introduced into the Italian legal system for the first time - governs the administrative liability of corporate bodies, companies and associations, including those without legal personality.

Particularly, Delegated Law 300/2000, which also ratifies the convention of July 26, 1995 on the financial protection of the European Communities, the EU convention of May 26, 1997 on the fight against corruption and the OECD convention dated December 17, 1997 on combating bribery of foreign public officials in international business transactions, complies with the obligations set forth in said international instruments, and especially community ones, which in fact provide for the paradigms of liability of legal entities and a system of sanctions aimed at fighting corporate crimes.

Legislative Decree 231/2001 is therefore made in the context of implementing international obligations and - in line with the regulatory systems of many European countries - introduces the liability of a corporation ("Entity") considered to be "an independent center of interests and legal relationships, a point of reference for various types of precepts and where decisions are made and activities are performed by subjects operating on behalf and in the interest of the Entity".

The establishment of the administrative liability of Entities is based on the empirical consideration that often illegal acts committed within the organization are not so much an expression of the deviant behavior of the individual but rather of that found in the center of economic interests in which the individual acted, often resulting from decisions made by the top management of said center. It is therefore believed that said criminal behavior can only be effectively prevented by also punishing the Entity, which is the real beneficiary of the offence.

Regarding the real nature of the liability as per Legislative Decree 231/2001, it appears to combine the features of both administrative and criminal liability. The ministerial report on the Decree, in fact, underscores the fact that this type of liability, resulting from an offence and tied to the guarantees of a criminal trial, differs in various points from the traditional paradigm of an administrative offence and presents itself as an independent type of liability that "combines the essential features of the penal and administrative systems in an attempt to reconcile effective prevention measures with the even more fundamental principles of providing the maximum guarantee".

In particular, Legislative Decree 231/2001 provides for a well-structured system of sanctions ranging from the milder pecuniary sanctions to the harsher penalty of disqualification, including the "capital" penalty of being disqualified from running a business.

The administrative sanctions provided for in the Decree can in fact only be applied by a criminal court under the safeguards of a criminal trial, only if all the objective and subjective requirements laid down by the legislature exist: an offence has been committed by qualified individuals (top management figures or their subordinates) in the interest or for the benefit of the Entity .

An Entity is administratively liable in the following cases:

- an offence has been committed in the interest of the Entity or any time illegal conduct takes place with the sole intention of benefiting the Entity;
- the Entity has indirectly received an advantage from illegal conduct (economic or other) even though the person who committed the offence did not act with the sole intention of benefiting the Entity.

On the contrary, if the advantage is solely for the benefit of the agent (or of a third party to the Entity) this excludes the Entity's liability as its situation would be absolutely and clearly unrelated with the offence that was committed. Interest should also be construed objectively, placing emphasis on the final objective of the conduct (as stated in a recent case tried by the Court of Cassation, ref. Cass. Pen., Sez. II, sent. N. 295/2020), whereas the advantage is characterized as a set of benefits - especially property-related benefits - deriving from the offence and can be evaluated after the offence has been committed.

As regards the subjects, in Article 5 of Legislative Decree 231/2001 the legislature states that the Entity is liable if the offence is committed:

- "by people occupying positions of representation, administration or management of the Entity or of one of its financially and functionally independent subsidiaries and by people exercising management and control of the company, de facto or other" (so-called top management figures);

- "by people under the management or supervision of one of the figures mentioned in letter a)" (so-called subordinates[1]).

For the purpose of establishing the Entity's liability, in addition to the existence of the afore-mentioned requirements that make it possible to objectively connect the offence to the Entity, the legislature also requires that the Entity's guilt be ascertained. This subjective requirement is associated with organizational blame understood as a violation of the Entity's self-imposed rules to prevent the offences in question. On the other hand, it is not necessary to identify or charge the natural person who committed the offence, nor is it necessary for the offence to be extinguished for reasons other than amnesty: in such cases, this is without prejudice to the Entity's liability provided that the requirements laid down by the law are fulfilled.

The liability of Entities is also extended to offences committed abroad, provided that the country in which the crime is committed does not bring legal action against the Entity, provided again that the particular conditions set forth in Legislative Decree 231/2001 are fulfilled.

The global nature of financial markets - which has never been so pronounced - as well as the Group's organization, which includes various controlled companies operating abroad, make it of primary importance to verify the extraterritorial jurisdiction of the punitive laws in place to monitor the rules that govern business in general and those found in Legislative Decree 231/2001, of which therefore the essentials should be described.

Legislative Decree 231/2001 contains a provision (Article 4 of the Decree) based on a moderate principle of universal jurisdiction according to which an Entity whose head office is in Italy can be liable for having committed one of the predicate offences mentioned in the List of Crimes 231, even if consummated entirely abroad. In particular, paragraph 1 of Article 4 above provides that the Entity is administratively liable in all cases where, for predicate offences committed abroad, the natural person who committed the offence also has to be punished pursuant to Articles 7, 8, 9 and 10 of the Criminal Code.

In order for an Italian judge to exercise his or her jurisdiction and apply to the Entity the administrative sanctions set forth in the Decree, in the case of offences committed abroad, the following specific conditions have to be met:

- the offence has to have been committed abroad (and completely consummated abroad) by an individual qualified as a "top management figure" or "subordinate");

[1]Subordinates are employees and also individuals who, although not subordinate to the Entity, have a relationship with the Entity that requires them to be monitored by the Entity's top management figures: some examples are agents, partners in joint ventures, para-subordinates in general, dealers, suppliers, consultants and collaborators.

- the Entity's head office has to be located in Italy (Articles 2196 and 2197 of the Civil Code);
- one of the conditions described in Articles 7[2], 8[3], 9[4] and 10 of the Criminal Code[5] has to be fulfilled;
- the Country in which the crime was perpetrated does not bring action against the Entity;
- in cases where the law provides that the guilty party is to be punished on the request of the Minister of Justice, action is brought against the Entity only if the request is also extended to said Entity.

Exceptions to the legislation in question are the so-called cross-border crimes under Law 146/2006, for which the criteria set forth in Article 4 of the Decree are not applicable, since they contain by nature an element of transnationality and can always be prosecuted by the Italian Judicial Authority.

Finally, note that the extension of liability under Article 4 of Legislative Decree 231/2001 only concerns those entities whose head offices are located in Italy. In order to determine the scope of this criterion in regard to businesses, reference must be made to civil law (Articles 2196 and 2197 of the Civil Code) to distinguish between the head office and branch offices, and concerning the obligation of companies to specify the location of their head office if they have more than one site. Should any discrepancies arise between the official data and the substantial data, or in the case of a failure to officially provide the information, the company's head office will be where the "company's center of administration, management and organization offices are located "(i.e. the actual headquarters according to Article 46 of the Civil Code).

1.1. PENALTIES APPLICABLE TO THE ENTITY

The penalties under Legislative Decree 231/2001 applicable to Entities for having committed or attempted to commit the afore-mentioned offences are:

- pecuniary penalties applied in quotas of not less than one hundred and not more than one thousand (the amount of the quota goes from a minimum of €250.00 to a maximum of €1,549.00) for a total ranging from a minimum of € 25,800 up to a maximum of € 1,549,000;

[2]Pursuant to Article 7 of the Criminal Code (**Offences committed abroad**):

1. *A citizen or foreigner is punishable under Italian law if he or she commits any of the following offences in a foreign country:*
   1. *offences against the security of the Italian State;*
   2. *offences involving the counterfeiting of the State seal and use of a counterfeit seal;*
   3. *offences involving the forgery of the State's legal tender or revenue stamps or Italian bearer bonds;*
   4. *offences committed by public officials in the service of the State, who abuse their power or fail to fulfill the duties of their roles;*
   5. *any other offence for which special statutory provisions or international conventions establish the applicability of Italian criminal law*

[3]Pursuant to Article 8 of the Criminal Code. (**Political offence committed abroad):**

1. *A citizen or foreigner is punishable under Italian law on the request of the Minister of Justice if he or she commits a political offence not included among those listed in item 1 of the previous article.*
2. *If the offence is punishable because of an action brought by the injured party, in addition to this request, the complaint must also be produced.*
3. *For the purposes of criminal law, a political offence is any offence that damages a political interest of the State or a citizen's political right. A common offence committed entirely or partially for political reasons is also considered a political offence.*

[4]Pursuant to Article 9 of the Criminal Code. **(Common offence committed by citizens abroad**):

1. *Aside from the cases indicated in the two previous articles, any citizen who commits a crime in a foreign country, which according to Italian law is punishable by death or a life sentence or a prison sentence of not less than three years, is punished according to said law provided he or she is in the Country.*
2. *In the case of an offence entailing the application of a penalty involving short-term deprivation of personal freedom, the guilty party is punished on the request of the Minister of Justice or on the petition or complaint of the injured party.*
3. *In the cases set forth in the previous provisions, in the case of an offence committed to the detriment of the European Communities, foreign State or foreigner, the guilty party is punished on the request of the Minister of Justice, provided that his or her extradition has not been granted or has not been agreed to by the Government of the Country in which he or she committed the crime.*

[5]Pursuant to Article 10 of the Criminal Code. **(Common offence committed abroad by a foreigner):**

1. *Any foreigner who, aside from the cases indicated in Articles 7 and 8, commits a crime in a foreign country to the detriment of the State or a citizen, which according to Italian law is punishable by death or a life sentence or a prison sentence of not less than one year, is punished according to said law provided he or she is in the Country and the request comes from the Minister of Justice or from a petition or complaint of the injured party.*
2. *If the offence is committed to the detriment of the European Communities, a foreign State or foreigner, the guilty party is punished according to Italian law on the request of the Minister of Justice, as long as:*
   1. *he or she is in the Country;*
   2. *the offence carries a death sentence or a life sentence or a prison sentence of not less than three years;*
   3. *his or her extradition has not been granted or has not been agreed to by the Government of the Country in which he or she committed the crime or by the Country to which he or she belongs.*

- interdictory sanctions[6] (also applicable as precautionary measures) for a period of not less than three months and not exceeding two years[7], which, in turn, may consist of:
  - business prohibition;
  - suspension or revocation of authorizations, licenses or concessions that could enable a crime to be committed;
  - prohibition on contracting with the Public Administration;
  - exclusion from incentives, loans, grants or subsidies and possible revocation of the ones that have already been granted;
  - prohibition on advertising of goods or services;
- confiscation of the price of or the profits from the crime (or precautionary seizure);
- publication of the ruling (if an interdictory sanction is applied).

Interdictory sanctions are only applied to crimes for which they have been explicitly specified and as long as at least one of the following conditions is fulfilled:

- the Entity earned a significant profit from the crime and the crime was committed by top management figures or by subordinates if in the latter case the perpetration of the crime was due to or facilitated by serious organizational shortcomings;
- repetition of the offences.

Notwithstanding the application of pecuniary sanctions, interdictory sanctions are not applicable if prior to the start of the opening statements of the trial of first instance, the following conditions have been fulfilled[8]:

a) the Entity has fully compensated the damage and eliminated the damaging or dangerous consequences of the crime, or has made an effective effort in this respect;

b) the Entity has eliminated the organizational shortcomings that determined the crime by adopting and implementing organizational models to prevent crimes like the one that was committed;

c) the Entity has allowed the earned profits to be confiscated.

The Decree also provides that in the more serious cases the judge may order a definitive business prohibition if the Entity earned a considerable profit from the crime and has already been sentenced to a temporary business prohibition at least three times in the last seven years.

The judge may also hand down a definitive prohibition on contracting with the Public Administration or a prohibition on the advertising of goods or services if this sanction has already been applied to the Entity at least three times in the last seven years.

If the Entity or one or its organizational units is consistently used for the sole or prevailing purpose of allowing or facilitating the perpetration of crimes for which the Entity is liable, a definitive business prohibition will always be ordered.

[6]The sanctions are strictly those set forth in Article 9, paragraph 2 of Legislative Decree 231/2001.
[7]With the exception of what is stated in Article 25, paragraph 5 of Legislative Decree 231/2001.
[8]Article 17 of Legislative Decree 231/2001.

If the crimes indicated in Section I of Legislative Decree 231/2001 are only attempted, the pecuniary sanctions (in terms of the amount) and the interdictory sanctions (in terms of time) are reduced by a one third to one half, whereas sanctions are not imposed in cases where the Entity voluntarily prevents the action from being carried out or the event from occurring.

1.2. EXEMPTION FROM LIABILITY: ORGANIZATION, MANAGEMENT AND CONTROL MODEL

Articles 6 and 7 of Legislative Decree 231/2001 explicitly state that an Entity is exempt from administrative liability if it has actually and effectively adopted organization and management models to prevent crimes of the type that took place. Proper organization is therefore the only instrument able to negate the Entity's "guilt", and consequently exclude the application of penalties to said Entity.

Specifically, liability is excluded if the Entity proves that:

a) prior to the crime being committed, the board of directors adopted and effectively implemented the appropriate "organization, management and control models to prevent crimes of the type that were committed;

b) the responsibility of monitoring the models to make sure they are properly applied and complied with, and to keep them up to date, has been entrusted to one of the Entity's bodies vested with independent powers of initiative and control;

c) people committed the crime by fraudulently circumventing the organization and management models;

d) the body indicated in letter b) did not fail to monitor and was not remiss in monitoring.

The adoption of a Model that is specifically designed for the risks to which the Entity is exposed, aimed at preventing certain crimes from being committed by establishing rules of conduct, therefore constitutes the measure of diligence established by the legislature, and represents - because of its preventive function - the first system check on risk control.

The mere adoption of the Model by the managing body - which is the body vested with management power: the Board of Directors - does not however appear to be sufficient to determine an exemption from liability for the Entity, as the Model also has to be effective and in force.

As for the effectiveness of the Model, the legislature, in Article 6, paragraph 2 of Legislative Decree 231/2001, dictates that the Model has to comply with the following requirements:

1. identify activities where crimes could be committed (the so-called "mapping" of at-risk activities);

2. provide for specific protocols aimed at planning training and implementing the Entity's decisions concerning the crimes to be prevented;

3. determine how to manage financial resources to prevent crimes from being committed;

4. establish obligations to provide information to the body tasked with monitoring the operation of and compliance with the models

The Model's effectiveness is instead tied to its actual implementation which, according to Article 7, paragraph 4 of Legislative Decree 231/2001, requires:

1. a periodical check and possible amendment to the Model if significant violations of the provisions are discovered, or if there are changes in the organization or in the business (updating the Model);

2. a disciplinary system to punish non-compliance with the measures set forth in the Model
3. suitable initiatives for personnel education and training.

Nonetheless, the adoption of a Model does not constitute an obligation for Entities but merely a right, which, however, allows them to benefit from the exemption from liability and other advantages in terms of reduced sanctions.

2. ADOPTING THE ORGANIZATION, MANAGEMENT AND CONTROL MODEL

2.1 Model Structure

This Model comprises a general section and individual special sections referring to the various types of crimes provided for in the Decree, as follows:

- Special Section "A": applicable to specific types of crimes committed to the detriment of the Public Administration, as per art. 24 and 25 of the Decree, and to private-to-private corruption.
- Special Section "B": applicable to corporate crimes as per art. 25 *ter* of the Decree (excluding the crime of private-to-private corruption) and to administrative crimes and offences such as internal dealing and market manipulation, as per art. 25 *sexies* of the Decree.
- Special Section "C": applicable to the crimes of manslaughter and unintentional serious or very serious injury in violation of the obligations to safeguard health and safety in the workplace (art. 25 *septies* of the Decree).
- Special Section "D": refers to computer-related crimes and illegal processing of data, as provided for in article 24 *bis* of the Decree.
- Special Section "E": deals with money laundering, possession of stolen goods, and use of illegal money, goods or advantages (art. 25-*octies* of the Decree) and crimes involving non-cash payment instruments (art. 25-*octies* 1 of the Decree).
- Special Section "F": refers to crimes by criminal organizations as per art. 24 *ter* of the Decree, and to transnational crimes (as per art. 10 of Law n. 146/2006).
- Special Section "G": deals with environmental crimes as per art. 25 *undecies* of the Decree.
- Special Section "H": deals with areas of business in which the crime of smuggling could be committed, pursuant to article 25 *sexiesdecies* of the Decree.

The Model also has an Appendix containing the following:

- "Transactions set up directly and "not according to procedure" by top management figures. This document sets out the specific elements of control with which the Company's top management figures must comply whenever they are about to begin or are beginning transactions that follow a procedure other than the one specified in the Model, due to exceptional situations of extraordinary urgency or particular situations of confidentiality or even because of the particular nature of the transaction;
- "General principles of internal control ", which establish all the "mechanisms" to be used to reach the targets of operating efficiency and effectiveness, reliability of financial and operating information, compliance with laws and regulations, and safeguarding of assets against possible fraud;

- "Principles of conduct with the Public Administration", describing the behavioral guidelines the Company must follow to prevent the creation of any situations that are conducive to the perpetration of the crimes set forth in the Decree;

- "Compatible public entities according to Legislative Decree n. 231/2001", which contains a summary including but not limited to the entities which should be considered public.

FATA's Board of Directors has the right to make additions to this Model by means of a resolution if crimes are introduced that are potentially connected with FATA's business.

2.2 Recipients of the Model

The "Recipients" of this Model who, as such and because of their specific duties, have the obligation to know and comply with the Model, are the members of the Board of Directors and the Board of Statutory Auditors, Executives, Employees and all the collaborators with whom there is a contractual relationship of any kind, including occasional or even only temporary agreements, as well as anyone with any type of commercial or financial relations with FATA.

2.3 Predicate offences for which it is felt there is a risk of a crime being committed: List of cases

Crimes under art. 24 of the Decree (Fraud against the Public Administration):

Art. 316 *bis* of the penal code - Misappropriation of public funds;

Art. 316 *ter* of the penal code - Undue receipt of public funds;

Art. 356 of the penal code - Procurement fraud;

Art. 640, par. II, n. 1 of the penal code - Fraud to the detriment of the State;

Art. 640 *bis* of the penal code - Aggravated fraud for the purpose of obtaining public funds;

Art. 640 *ter* of the penal code - Computer fraud.

Crimes under art. 24 bis of the Decree (Cyber Crimes):

Art. 491 *bis* of the penal code - Computer documents;

Art. 615 *ter* of the penal code - Illegal access to IT or telematic systems;

Art. 615 *quater* of the penal code - Illegal possession, distribution and installation of equipment, codes and other means to access IT or telematic systems;

Art. 615 *quinquies* of the penal code - Possession, distribution and installation of computer equipment, devices or programs aimed at damaging or interrupting an IT or telematic system;

Art. 617 *quater* of the penal code - Illegal wiretapping, hindering or interruption of IT or telematic communication;

Art. 617 *quinquies* of the penal code - Illegal possession, distribution and installation of equipment and other means for the purpose of wiretapping, hindering or interrupting IT or telematic communication;

Art. 635 *bis* of the penal code - Damage to information, data or computer programs;

Art. 635 *ter* of the penal code - Damage to information, data or computer programs used by the State or other Public Entity, or that in any event are of service to the public;

Art. 635 *quater* of the penal code - Damage to IT or telematic systems;

Art. 635 *quinquies* of the penal code - Damage to public service IT or telematic systems;

Art. 640 *quinquies* of the penal code - Computer fraud against the entity that provides a certified e-mail service.

Crimes under art. 24 ter of the Decree (Organized Crime):

Art. 416, par. 6 of the penal code - Criminal conspiracy for the purpose of enslavement, human trafficking or purchase or sale of slaves;

Art. 416 of the penal code - Criminal conspiracy;

Art. 416 *bis* of the penal code - Mafia-type conspiracy;

Art. 416 *ter* of the penal code - Election rigging involving politicians and the mafia.

Art. 630 of the penal code - Kidnapping for extortion purposes;

Art. 416 *bis* of the penal code - Crimes committed by mafia-imposed subjugation and code of silence.

Art. 74 of Presidential Decree n. 309/1990 - Conspiracy to illegally traffic in narcotics or psychotropic drugs;

Art. 407, par. 2, lett. a) n. 5 of the penal code - Illegal manufacture, import, sale, transfer, possession and bearing, in places that are public or open to the public, of military weapons or parts thereof, explosives, illegal weapons and several common firing weapons.

This group also includes criminal conspiracies (articles 416 and 416 *bis*) or so-called transnational crimes as per Law n. 46/2006.

Crimes under art. 25 of the Decree (Embezzlement, illegal abuse of position, undue inducement to give or promise advantages, bribery and abuse of office):

Art. 314, par. 1 of the penal code – Embezzlement;

Art. 316 of the penal code - Embezzlement by profiting from the mistakes of others;

Art. 317 of the penal code - Illegal abuse of position;

Art. 318 of the penal code - Bribery of a public official;

Art. 319 of the penal code - Bribery of a public official to make him/her act in a manner that is contrary to his/her official duties;

Art. 319 *bis* of the penal code - Aggravating circumstances;

Art. 319 *ter* of the penal code - Bribery in judicial proceedings;

Art. 319 *quater* of the penal code - Undue inducement to give or promise advantages;

Art. 320 of the penal code - Bribery of a public service officer;

Art. 321 of the penal code - Punishment of the briber;

Art. 322 of the penal code - Instigation to bribery;

Art. 322 *bis* of the penal code - Embezzlement, illegal abuse of position, bribery and instigation to bribe members of the European Community and officials of the European Community and foreign countries;

Art. 323 of the penal code - Abuse of office;

Art. 346-bis of the penal code – Influence peddling

Crimes under art. 25 ter of the Decree (Corporate Crimes):

Art. 2621 of the civil code - False accounting;

Art. 2621 *bis* of the civil code - Minor false accounting;

Art. 2622 of the civil code - False accounting to the detriment of the company, shareholders or creditors;

Art. 2625 of the civil code - Obstruction of audit;

Art. 2626 of the civil code - Undue return of capital contributions;

Art. 2627 of the civil code - Unlawful distribution of profits and reserves;

Art. 2628 of the civil code - Unlawful transactions involving shares or share capital or by the controlling company;

Art. 2629 of the civil code - Transactions that are detrimental to creditors;

Art. 2629 *bis* of the civil code - Failure to report conflicts of interest;

Art. 2632 of the civil code - Fictitious capital;

Art. 2633 of the civil code - Undue distribution of company assets by the liquidators;

Art. 2635 of the civil code - Bribery among private individuals;

Art. 2635 *bis* of the civil code - Instigation to bribery among private individuals;

Art. 2636 of the civil code - Undue influence in general shareholders' meetings;

Art. 2637 of the civil code - Market rigging;

Art. 2638 of the civil code - Preventing public supervisory bodies from performing their duties.

Crimes under art. 25 sexies of the Decree (Market Abuse):

Art. 183 of Legislative Decree n. 58/98 - Exemptions from criminal liability;

Art. 184 of Legislative Decree n. 58/98 - Crime of insider trading;

Art. 185 of Legislative Decree n. 58/98 - Crime of market manipulation;

Art. 187 *bis* of Legislative Decree n. 58/98 - Insider trading;

Art. 187 *ter* of Legislative Decree n. 58/98 - Market manipulation.

Crimes under art. 25 septies of the Decree (Workplace Safety):

Art. 589 of the penal code - Manslaughter;

Art. 590 of the penal code - Unintentional personal injury.

Crimes under art. 25 octies of the Decree (possession of stolen goods, money laundering, use of illegal money, goods or advantages, self-laundering;

Art. 648 of the penal code - Possession of stolen goods;

Art. 648 *bis* of the penal code - Money laundering;

Art. 648 *ter* of the penal code - Use of illegal money, goods or advantages;

Art. 648 *ter.1* of the penal code - Self-laundering.

Crimes under art. 25 octies. 1 of the Decree (crimes involving non-cash payment instruments):

Art.493-ter of the penal code - Illicit use and forgery of non-cash payment instruments

Art. 493-quater -Possession and distribution of computer equipment, devices or programs for the purpose of committing crimes involving payments instruments other than cash

Art. 640 ter, par. 2 of the penal code - Computer fraud aggravated by the transfer of money, monetary value or virtual currency

Crimes under art. 25 sexiesdecies of the Decree (Smuggling)

Presidential Decree 43 of January 23, 1973 (TUD - *Consolidated Law on Customs*).

Art. 282 TUD - Smuggling of goods through land borders and customs areas;

Art. 283 TUD - Smuggling of goods through lakes with international borders;

Art. 284 TUD - Smuggling of goods by sea;

Art. 285 TUD - Smuggling of goods by air;

Art. 286 TUD - Smuggling in duty-free areas;

Art. 287 TUD - Smuggling due to illegal use of imported goods with reduced customs duties;

Art. 288 TUD - Smuggling in customs warehouses;

Art. 289 TUD - Smuggling in cabotage and circulation of goods;

Art. 290 TUD - Smuggling in the export of goods subject to recovery of customs duties;.

Art. 291 TUD - Smuggling in temporary importing or exporting.

Crimes under art. 25 undecies of the Decree (Environmental Crimes):

Legislative Decree 152/2006 - Collection, handling, transport, recycling and disposal of waste, including hazardous waste, without the required authorizations, including the monitoring of these operations and inspection of disposal sites, as well as the activity of dealers or brokers;

Law 549/1993 - Violation of the regulations governing the production, consumption, import, export, possession, collection, recycling or marketing of stratospheric ozone depleting substances and of substances that are harmful to the environment.

Crimes under art. 25 duodecies of the Decree (Employment of third country nationals with irregular residence permits):

Legislative Decree 286/ 1998 and subsequent amendments and additions - Employment of third country nationals with irregular residence permits.

Crimes under art. 25 quinquiesdecies of the Decree (Tax Crimes):

Art. 2 of Legislative Decree 74/2000 - False declaration by means of invoices or other documents for non-existent transactions;

Art. 3 of Legislative Decree 74/2000 - False declaration by means of other artifices;

Art. 4 of Legislative Decree 74/2000 - False declaration in cases of serious cross-border VAT fraud;

Art. 5 of Legislative Decree 74/2000 - Non-declaration in cases of serious cross-border VAT fraud;

Art. 8 of Legislative Decree 74/2000 - Issuing of invoices or other documents for non-existent transactions;

Art. 10 of Legislative Decree 74/2000 - Concealment or destruction of accounting documents;

Art. 10-*quater* of Legislative Decree 74/2000 - Undue payment in cases of serious cross-border VAT fraud.

2.4 Predicate offences for which - depending on the company's business and work environment - the risk of a crime being committed is not considered conceivable but will nonetheless be monitored: List of cases.

Crimes under art. 25 bis of the Decree (forgery of currencies, bearer bonds, revenue stamps or tools or marks of identification);

Art. 453 of the penal code - Forgery of currencies, spending and bringing counterfeit money into the country by arrangement;

Art. 454 of the penal code - Altering currency;

Art. 455 of the penal code - Spending and bringing counterfeit money into the country without arrangement;

Art. 457 of the penal code - Spending of counterfeit money received in good faith;

Art. 459 of the penal code - Counterfeiting of tax stamps and bringing them into the country, purchase, possession or distribution of counterfeit tax stamps;

Art. 460 of the penal code - Counterfeiting of watermarked paper used to make bearer bonds and tax stamps;

Art. 461 of the penal code - Making or possession of watermarks or tools used for the counterfeiting of money, tax stamps or watermarked paper;

Art. 464 of the penal code - Use of counterfeit or altered tax stamps;

Art. 473 of the penal code - Counterfeiting, altering or use of distinctive trademarks or marks, or patents, models and drawings;

Art. 474 of the penal code - Bringing forged trademarks into the country and their trade.

Crimes under art. 25 bis.1 of the Decree (Crimes against industry and trade):

Art. 513 of the penal code - Disturbing the freedom of industry or trade;

Art. 513 *bis* of the penal code - Illegal competition involving threats or violence;

Art. 514 of the penal code - Fraud against national industries;

Art. 515 of the penal code - Fraud in trade;

Art. 516 of the penal code - Sale of non-genuine foodstuffs as genuine;

Art. 517 of the penal code - Sale of industrial products with deceitful markings;

Art. 517 *ter* of the penal code - Manufacture and trade of goods by infringing industrial property rights;

Art. 517 *quater* of the penal code - Counterfeiting of geographical indications or designations of origin of agri-foods.

Crimes under art. 25 quater of the Decree (Crimes for the purpose of terrorism or for the subversion of the democratic order):

Art. 270 - *bis* of the penal code - Conspiracy to commit national or international acts of terrorism or to subvert democracy;

Art. 270 - *ter* of the penal code - Conspiracy to commit international acts of terrorism;

Art. 270 - *quater* of the penal code - Recruitment for the purpose of committing national or international acts of terrorism;

Art. 270 - *quinquies* of the penal code - Training for the purpose of committing national or international acts of terrorism;

Art. 270 - *sexies* of the penal code - Conduct for the purpose of committing acts of terrorism;

Art. 280 of the penal code - Attacks of terrorism or subversion;

Art. 280 - *bis* of the penal code - Act of terrorism using lethal or explosive devices;

Art. 289 - *bis* of the penal code - Kidnapping for purposes of terrorism or subversion;

Art. 302 of the penal code - Instigation to commit some of the crimes listed in the first and second chapters [under the same title of the penal code];

Crimes under art. 25 quater - 1 of the Decree (Mutilation of female genitals):

Art. 583 *bis* of the penal code - Mutilation of female genitals.

Crimes under art. 25 quinquies of the Decree (Crimes against individuals):

Art. 600 of the penal code - Enslaving and keeping people in slavery or servitude;

Art. 600 *bis* of the penal code - Prostitution of minors;

Art. 600 *ter* of the penal code - Pornography involving minors;

Art. 600 *quater* of the penal code - Possession of pornographic material;

Art. 600 *quater* of the penal code - Virtual pornography;

Art. 600 *quinquies* of the penal code - Tourism initiatives for the exploitation of child prostitution;

Art. 601 of the penal code - Human trafficking;

Art. 602 of the penal code - Purchase or sale of slaves;

Art. 603 *bis* of the penal code - Illegal intermediation and exploitation of labour;

Art. 609 *undecies* of the penal code - Solicitation of minors.

Crimes under art. 25 novies of the Decree (Copyright infringement):

Art. 171 par. a *bis* Law 633/1941 - Making a protected original work or part of it public;

Art. 171 *bis* Law 633/1941 - Illegal copying of programs;

Art. 171 *ter* Law 633/1941 - Illegal use of original works or of intangible products, decoding devices or elements;

Art. 171 *septies* Law 633/1941 - Failure to provide SIAE with the data needed to unequivocally identify the media that do not require a SIAE sticker;

Art. 171 *opties* Law 633/1941 - Use, even by private individuals, of devices to decode audiovisual programs with restricted access, by means of wireless, satellite or cable systems.

Crimes under art. 25 decies of the Decree (Inducement to not make statements or to make false statements before the judicial authority).

Art. 377 *bis* of the penal code - Inducement to not make statements or to make false statements before the judicial authority.

Crimes under Law 146/2006 - Transnational Crimes:

Art. 377 *bis* of the penal code - Inducement to not make statements or to make false statements before the judicial authority;

Art. 378 of the penal code - Aiding and abetting;

Art. 291 *quater* of Presidential Decree 43/1973 - Conspiracy to smuggle foreign processed tobacco;

Art. 74 of Presidential Decree 390/1990 - Conspiracy to traffic illegally in narcotics or psychotropic drugs;

Art. 12, par. 3, 3 *bis*, 3 *ter* and 5 of Legislative Decree 286/1998 - Migrant smuggling.

The criminal conspiracies in articles 416 and 416 *bis* of the penal code have been included among the potentially committable crimes listed in paragraph 2.3.

Crimes under art. 25 undecies of the Decree (Environmental Crimes):

Art. 452 *bis* of the penal code - Environmental pollution;

Art. 452 *quater* of the penal code - Environmental disaster;

Art. 452 *quinquies* of the penal code - Unintentional environmental disasters;

Art. 452 *sexies* of the penal code - Trafficking in and dumping of highly radioactive material;

Art. 452 *bis* of the penal code - Aggravating circumstances;

Art. 727 *bis* of the penal code - Killing, destruction, capture, collection and possession of wild or protected animal and plant species;

Art. 733 *bis* of the penal code - Habitat damage;

Law 150/1992 - Import, export, sale, transport, including on behalf of third parties, possession of endangered animal and plant species;

Legislative Decree 202/2007 - Intentional and unintentional sea pollution.

Crimes under art. 25 terdecies of the Decree (Racism and xenophobia):

Art. 5 par. 3 - Racism and xenophobia.

Crimes under art. 25 quaterdecies of the Decree (Fraud in sporting events):

Art. 1, L. 401 of December 13, 1989 – Fraud in sports events;

Art. 4, L. 401 of December 13, 1989 – Illegal gambling or betting

Crimes under art. 25 septiesdecies of the Decree (Cultural Goods):

Art. 518 *bis* of the penal code - Theft of cultural goods;

Art. 518 *ter* of the penal code - Misappropriation of cultural goods;

Art. 518 *quater* of the penal code - Possession of stolen cultural goods;

Art. 518 *octies* of the penal code - Forgery of private documents related to cultural goods;

Art. 518 *novies* of the penal code - Violations in the alienation of cultural goods;

Art. 518 *decies* of the penal code - Illegal import of cultural goods;

Art. 518 *undecies* of the penal code - Illegal exit or export of cultural goods;

Art. 518 *duodecies* of the penal code - Destruction, loss, deterioration, defacement, staining and illegal use of cultural goods or cultural landscapes;

Art. 518 *quaterdecies* of the penal code - Forgery of works of art.

Crimes under art. 25 duodevicies of the Decree (Laundering, destruction and pillaging of cultural goods and cultural landscapes)

Art. 518 *sexies* of the penal code - Laundering of cultural goods;

Art. 518 *terdecies* of the penal code - Destruction and pillaging of cultural goods and cultural landscapes.

For a more detailed description of the predicate offences which fall within the scope of application of the Decree, please refer to the document in Attachment 2.

2.5 Approval and implementation of the Model's principles

Since the Model is a "document issued by the board of directors" [in compliance with the provisions of art. 6, par. I, lett. a) of the Decree], dated September 26, 2022, the Board of Directors of FATA S.p.A. approved the adoption of this document by updating the existing Model.

Likewise, subsequent substantial modifications and additions will be the responsibility of the above-mentioned Board of Directors.

3. ORGANIZATIONAL STRUCTURE OF FATA S.p.A.

The aspects of the pre-monitoring system that need to be implemented within the company to ensure the Model's effectiveness are:

- ethical principles aimed at preventing the crimes specified in the Decree;
- an adequately formalized and clear-cut organizational structure;
- manual or computerized operating procedures aimed at regulating activities in the company's areas of risk, together with the necessary check points;
- authorization and signatory powers consistent with organizational and management responsibilities;
- management control system able to promptly report the existence and the appearance of critical situations;
- personnel information and training system covering all the elements of the Model, including the Code of Ethics;
- disciplinary system to punish any violations of the Code of Ethics or of the other indications in the Model.

Described below are the principles on which certain protocols of the FATA Model are based, which have features in common with all the crimes indicated in the Decree, whereas - notwithstanding what is stated in this paragraph - for protocols with specific features for each type of crime (i.e. procedures or other specific protocols) please refer to the Special Sections.

As regards the Code of Ethics, Supervisory Committee, disciplinary system and personnel information and training system, please refer to the chapters in the Model that specifically deal with these matters.

Organizational System

The company's organizational system (organizational structure/positions, missions and areas of responsibility), currently specified in Attachment 3, is determined by the Organizational Provisions (Service Orders and Internal/Service Memos) issued by the Chairman and/or Chief Executive Officer. The Human Resources Department ensures that these provisions are formalized and distributed, as well as periodically updating the company's organization chart.

Based on the issued Organizational Provisions, a document is drawn up illustrating the company's organization chart and the missions and responsibilities of each organizational structure, which reflects the content of the Organizational Provisions and is distributed to all company personnel.

Service Orders may refer to:

- company guidelines, orientation and policy;
- formalization of company processes and procedures;
- establishment, modification, elimination of company boards, committees, projects and work groups.

The company may also issue and divulge internal/service memos referring to the organizational and operational aspects of the company.

Authorization System

The company's authorization system is set up according to the following requirements:

- delegations of powers and powers of attorney match the powers to the corresponding area of responsibility;
- each delegation of powers and power of attorney unequivocally determines the powers of the proxy, while specifying his or her limits;
- the management powers conferred by delegation / power of attorney are consistent with the company's goals;
- anyone acting on behalf of FATA in relations with third parties and especially with the Public Administration, shall possess a specific delegation of powers and/or a formal power of attorney authorizing them to represent the Company;

In particular, the following powers can be assigned:

- *enduring powers of representation*, assigned by means of registered, notarized powers of attorney based on the fulfillment of activities that fall within the permanent responsibilities of the company's organization;
- *powers for single projects*, conferred by means of notarized powers of attorney or other delegations of power depending on their content; the conferral of these powers is regulated by Company procedures and by the laws that establish the types of representation, depending on each document to be stipulated.

Company procedures in at-risk areas

Internal procedures shall include the following elements:

- separation, whenever possible and within each process, between the person making the decision (decision-making impulse), the person who authorizes it, the person who implements the decision and the person who monitors the process (referred to as "separation of duties);
- a written record of each step of the process, including checking (referred to as "traceability");
- suitable level of formalization.

Management control and financial flows

The management control system adopted by FATA covers various phases, i.e. preparation of the annual *budget*, periodical analysis of actual costs and drawing up forecasts for the Company.

The system ensures:

- the involvement of multiple people so that the duties of preparing and divulging information are properly separated;
- the ability to promptly report the existence or appearance of critical situations through suitable and timely information flows and *reporting*.

Financial resources are managed according to principles that are essentially characterized by a separation of duties, thus ensuring that all expenditures are requested, made and checked by independent individuals

or by different individuals whenever possible. Moreover, these individuals have not been assigned other responsibilities that could lead to potential conflicts of interest.

Finally, liquidity management is based on the principle of safeguarding the company's assets and not allowing risky financial transactions to take place, and may require two signatures for amounts above the established limits.

Document Management

All of FATA's internal and external documentation is managed according to procedures that regulate, depending on the case, the updating, distribution, recording, filing and security of documents and recordings.

Specific controls, including technical controls, prevent unauthorized individuals from gaining access, both incoming and outgoing, to the Company's protocol, making it impossible to modify existing protocols.

4. SUPERVISORY COMMITTEE

4.1 Supervisory Committee

The Decree (art. 6 lett. b) requires, as an additional condition for exemption from administrative liability, that the duty of monitoring the operation of and compliance with the Model as well as updating it, be assigned to a Company body vested with independent powers of initiative and control.

According to the spirit of the regulation and the latest Guidelines issued by Confindustria, this is a multi-member body referred to as a "Supervisory Committee" whose members must possess the requirements of:

- autonomy and independence;
- professionalism;
- continuous action;
- good standing.

Considering the particular responsibilities and specific professional skills required to perform its tasks of monitoring and control, the Supervisory Committee may in any case avail itself of other internal personnel or external collaborators under its direct supervision and responsibility, who may be needed depending on the specific tasks assigned in each case.

4.2 Regulation on appointing, removing and replacing members of the Supervisory Committee

Also considering the latest indications added to the *"Guidelines to set up organization, management and control models pursuant to Legislative Decree 231/2001"* issued by Confindustria, FATA has assigned the Supervisory Committee the following duties, regulating its operation as described below, notwithstanding the Supervisory Committee's power-duty to independently regulate its operation and activities, even by modifying these provisions if necessary.

The choices made by the Supervisory Committee cannot be challenged by the Company's institutions as this would invalidate the Committee's essential requirement of independence.

4.3 Composition of the Supervisory Committee

During the meeting of September 14, 2018, FATA's Board of Directors approved the current rules of procedure for the Supervisory Committee (hereinafter "**Committee**"), made up of FATA's *pro-tempore*

head of Legal Affairs and two external independent members since this composition is considered to be suitable for the type of activity required.

The Supervisory Committee shall comprise multiple members, namely the head of the legal department of each company and two external members; the position of Committee Chairman shall be held by one of the two external members. Each member of the Supervisory Committee shall guarantee the requirements of autonomy and independence.

The appointment of the Supervisory Committee shall be submitted to the company's Board of Directors for approval.

4.4 Term of Office

The Committee Chairman shall remain in office for three years. The term can be renewed only once and the Chairman shall in any event remain in office until a successor has been appointed. The members of the Committee shall remain in office for three years. Their term can be renewed and they shall in any event remain in office until a successor has been appointed.

The members' term in office can also come to an end following resignation, dismissal or revocation.

The Committee members can resign at any time, and FATA's Board of Directors and Board of Statutory Auditors shall be notified in writing of their resignation. The Board of Directors shall make the necessary decisions as per the Rules of Procedure of the Committee.

4.5 Appointment, revocation and suspension of the Supervisory Committee

At the end of each term of office of the Committee and before any new appointments, the Board of Directors shall make sure that each Committee member possesses the requirements explicitly specified in the Decree, as well as the other requirements mentioned in this Model.

The Board of Directors periodically evaluates the suitability of the Committee in terms of organizational structure and conferred powers. The Board of Directors may also at any time, as specified in the Committee's Rules of Procedure, remove from office one (or all) of the members of the Committee, if the requirements of autonomy and independence, professionalism and continuous action in the performance of duty are no longer valid, or for reasons of incompatibility of the Committee members, or in the other cases stated in the Committee's Rules of Procedure.

In the case of resignation, incapacity, death, revocation or dismissal of one of its members, the Committee shall promptly notify the Board of Directors, which shall replace the member without delay. The Chairman of the Committee, or its most senior member, has the obligation to promptly notify the Board of Directors of any occurrence that would require the replacement of a Committee member.

In the case of resignation, incapacity, death, revocation or dismissal of the Chairman, the most senior member shall replace him/her, and shall remain in office until the date on which the Board of Directors appoints a new Chairman.

The Board of Directors, after having consulted with the Board of Statutory Auditors and the other members of the Committee, may decide to suspend a Committee member from office, in the cases and according to the procedures set forth in the Rules of Procedure of the Committee.

4.6 Duties and powers of the Supervisory Committee

The Supervisory Committee has the following duties:

- to oversee the effectiveness of the Model, i.e. ensure that the conduct within the company complies with the Model;
- to verify the effectiveness of the Model, i.e. verify that the Model is in fact able to prevent crimes from being committed;
- to make proposals to maintain and update the Model so that it is always in line with any changes to the corporate business and structure, and with any changes in legislation;
- to make Model amendment proposals to the corporate boards/departments that are able to implement them within the company.

The Committee shall therefore:

- periodically verify the map of the areas that are at risk of a crime being committed, adjusting it according to the changes in company business and/or structure, and to any changes in legislation. To this end, the *management* figures and control officers of all departments shall inform the Committee of any situations that could expose the company to a crime risk;
- perform periodical inspections based on a yearly schedule drawn up in advance to ascertain that the provisions of the Model have been fulfilled.

In particular, the Committee shall make sure that:

- the control procedures are in place and properly documented;
- the ethical principles are being complied with;
- the Model is suitable and effective in preventing the crimes set forth in the Decree;
- it works with the company departments (including in meetings):
  - to exchange information and keep the crime risk areas up to date;
  - to keep changes under control with a view to constant monitoring;
  - on the various aspects pertaining to Model implementation (standard contractual clauses, personnel training, changes in regulations and organization, etc.);
  - to ensure that the necessary corrective actions are promptly taken to make the Model suitable and effective;
- to collect, prepare and keep all the significant information received concerning compliance with the Model, and to update the list of information to be sent to the Committee;
- to make available and update on the company intranet the information concerning the Decree and the Model.

The Committee shall have free access to all company documentation and the possibility of acquiring significant data and information from managers, as well as ensuring that the heads of company departments promptly provide the information, data and/or news requested of them without restriction and without the need for prior consent.

In addition to the collaboration of specifically delegated company departments, the Supervisory Committee may also avail itself of external consultants who possess the requirements of professionalism and reliability needed to carry out a supervisory activity, and if necessary, may hear Employees, Directors and members of the Board of Statutory Auditors of the Company.

The Committee shall also have the necessary financial resources proposed by the Committee itself, and shall use them for anything that is required to properly perform their duties. To this end, FATA's Board of Directors shall allot the necessary funds when preparing the company budget.

4.7 Obligation to report to the Supervisory Committee

According to art.6, par. 2, letter d), of Legislative Decree 231/2001, one of the requirements of the Model is the "*obligation to provide information to the committee in charge of monitoring the operation of and compliance with the models*".

The Supervisory Committee shall be informed by the Recipients of the Model as to any events that could entail liability according to the Decree, or that could in any event constitute a violation of the Model's provisions. Moreover, any document reporting these circumstances shall be sent to the Supervisory Committee.

In particular, the Company enlists the Department Heads to implement the Model's provisions more effectively and practically. The Department Heads are responsible for operations in all the company's business areas where there is a potential risk of crimes being committed. The Department Heads shall be officially assigned the following tasks:

- to ensure for themselves and for the Recipients under their management and supervision, that the principles and rules of conduct set forth in the Code of Ethics are complied with and applied, as well as those of the other procedures, internal regulations, the Model and the Protocols;

- to assist the Supervisory Committee in carrying out the duties and activities associated with the responsibilities it has been given, interacting with the Committee and ensuring periodical information flows through verification and control activities.

An obligation to report to the Supervisory Committee has therefore been established in the form of **information flows set up** in the Model, which contain information, data and news concerning adherence to the principles of control and conduct specified in the Model, the Code of Ethics and the Protocols. The company structures involved in potentially at-risk activities shall then send this information to the Supervisory Committee, according to the timeframes and procedures established and notified by the Supervisory Committee itself. These flows are divided into:

- **Periodical information flows** addressed to the Supervisory Committee at regular intervals by the Department Heads involved in the at-risk activities as per Legislative Decree 231/2001, which, through a complete self-diagnostic process of the company's situation and business, show the level of implementation of the Model with particular attention to compliance with the procedures and internal regulations.

  Through this formal self-evaluation, they highlight the critical points of managed processes as well as any deviations from the indications of the Model and/or Protocols or of the regulatory framework in general, and the suitability of the actual regulations, while illustrating the actions and initiatives that have been adopted or planned to solve them.

  The Department Heads shall submit their statements to the Supervisory Committee within 15 days after the end of the half year. The 231 contact person shall file the documentation and make it available to the Supervisory Committee for which it shall prepare a report containing the results.

  The periodical information flows shall be sent to the Supervisory Committee at the following e-mail address: odv@fatagroup.it, indicating periodical information flow as the subject of the e-mail.

- **Information flows according to Attachment 5**, addressed to the Supervisory Committee by all the Recipients of the Model upon the occurrence of a single event, as specified in the Protocols of the Special Section.

These flows shall show all the information, data, news, reports or documents that the Special Section Protocols specify must be sent to the Supervisory Committee within the required timeframe. The information flows based on Attachment 5 shall be sent to the Supervisory Committee at the following e-mail address: odv@fatagroup.it, indicating information flow as per Attachment 5 as the subject of the e-mail.

In addition to the established information flows, according to art. 6, par. 2 *bis* of Legislative Decree 231/2001, one of the requirements of the Model is that*, for the purpose of safeguarding the company,* it has to provide *one or more channels* for the Model's Recipients to submit ***detailed reports*** *of illegal conduct as per Legislative Decree 231/2001, which are founded on precise, concordant facts, or of violations of the Model of which they became aware through the performance of their duties* [9] (i.e. occasional reports).

Finally, added to the types of information flows indicated in the Model and the occasional flows mentioned above are the **information flows to be provided upon the request of the Supervisory Committee**, which is any information specifically requested by the Supervisory Committee because it is considered significant for the monitoring of the Company's efficiency and effectiveness and to update the Model.

In fact, the Supervisory Committee, within the scope of its independent powers of initiative and control, may determine additional information flows for the purpose of obtaining other information of interest, identifying the content and level of detail, and then requesting the involvement of the pertinent company departments (including but not limited to the company departments involved in the "at-risk" areas listed in the Special Section of the Model).

As stated in art.6 par. 2 *bis* of Legislative Decree 231/2001, all the reporting channels guarantee that right from the moment the report is received and in each subsequent phase, the whistleblower's identity will remain confidential[10].

In general, reports shall preferably be in writing and sent to the Supervisory Committee through one of the following communication channels:

- **an information channel** accessible only to the Supervisory Committee to ensure that the whistleblower's identity remains confidential (preferred channel), which the Company undertakes to make known to all the Recipients;
- **a physical address** where the report can be sent in a closed, sealed envelope with the writing "reserved/personal" on the outside: FATA S.p.A. - Supervisory Committee, Strata Statale n. 24 km 12 - 10044 - Pianezza (Torino).

As an alternative, the whistleblower can request an audience with the Supervisory Committee to give his/her report verbally. This procedure requires that a written record be made of the report.

Only if the report refers to the conduct of a member of the Supervisory Committee or of the entire Committee, shall the whistleblower report directly to the company's board of directors. This procedure requires that the board of directors appoint an officer to deal with the report.

[9] Law 179 of November 30, 2017, added par. 2 *bis* to art. 6 of Legislative Decree 231/2001, regulating the "*Protection of employees or collaborators who report offences in the private sector"*.

[10] As pointed out in the "Guidelines on protecting public employees who report offences (so-called whistleblowers)" issued by ANAC with Decision n. 6 of April 28, 2015, "*the guarantee of confidentiality assumes that the whistleblower will reveal his/her identity. (...) This regulation essentially aims to ensure the protection of the employee by keeping his/her identity confidential only if the reports are from public employees who can be identified and recognized. It is, however, understood (...) that the Authority will also consider anonymous reports if they are given with sufficient detail and specifics, or if they can bring out facts and situations and link them to a given context*."

The Supervisory Committee or the officer in charge of dealing with the report shall assess the reports and information received and any resulting initiatives to be implemented in compliance with the internal disciplinary system and, if necessary, will hear the reporting person and/or the alleged perpetrator of the violation and then put down any decision in writing as well as proceeding with all the necessary verifications and inquiries.

Notwithstanding the above, the Supervisory Committee or the Officer in charge of dealing with the report shall also evaluate the anonymous reports provided that they too are suitably detailed and founded on *precise, concordant facts*, whereas any reports that are clearly not pertinent, not sufficiently detailed or defamatory will not be taken into consideration and will be immediately dismissed.

All information, documentation and reports referred to in this Model are stored in a specific database (soft or hard copy) by the Supervisory Committee or by the officer in charge of the reports for a period of 10 years; the Supervisory Committee or the Officer in charge of the reports shall keep the documents and information confidential, also in compliance with the privacy regulations. Access to the database is strictly limited to the Supervisory Committee.

The law[11]specifically prohibits any acts of direct or indirect reprisal or discrimination towards the whistleblower for reasons related either directly or indirectly to the report. The Supervisory Committee or other Officer in charge of the report shall therefore act in such a way as to protect the whistleblowers against any form of reprisal, discrimination or penalization, while ensuring the utmost confidentiality as to the identity of the whistleblower and as regards any news, information or report, under penalty of a specific sanction being applied, notwithstanding the requirements of any investigation, should it be necessary to request the assistance of consultants external to the Supervisory Committee or of other company boards.

The application of discriminatory measures towards anyone who makes a report as per par. 2 *bis* of art. 6 of Legislative Decree 231/2001 can be reported to the National Labour Inspectorate - which will act on matters over which it has authority - by the whistleblower and by the union indicated by him/her[12].

Retaliatory or discriminatory dismissal of the whistleblower is invalid.

Also invalid are any changes in duties as per art. 2103 of the civil code and any other retaliatory or discriminatory measure against the whistleblower.

In the case of disputes connected with any disciplinary sanctions, demotion, dismissal, transfer or subjecting the whistleblower to another organizational measure having a negative direct or indirect impact on work conditions following the submission of the report, the employer is responsible for proving that said measures are founded on reasons that are unrelated to the report.

4.8 Reporting to the company boards by the Supervisory Committee

The Supervisory Committee periodically reports to the Chairman and CEO and to the Board of Directors and the Board of Statutory Auditors, concerning the implementation of the Model and the occurrence of any critical points related thereto.

With particular reference to the type of *reporting*, the Supervisory Committee shall promptly report to the Chairman and CEO any violation of the Model considered to be well-founded, that was reported to the Committee by an employee or that the Committee itself has ascertained.

[11] Art. 6 par. 2 *bis* lett. c) of Legislative Decree 231/2001
[12] Art. 6 par. 2 *ter* of Legislative Decree 231/2001

The Supervisory Committee periodically submits its program of activities for the subsequent period to the company boards.

For the purposes of Model implementation, the Committee may also at any time ask the Auditing Company for information concerning any significant news it may have obtained during its activities.

5. TRAINING AND COMMUNICATION

For the purposes of Model implementation, personnel training and distribution of the document are handled by the Human Resources Department in close collaboration with the Committee, as follows:

- Management personnel with company representation duties: induction course on the general content of the Model, set-up of the Supervisory Committee and instructions on how to use the reporting channels. Occasional e-mail updates.
- Other staff: internal memos. Occasional e-mail updates.
- New employees: when they are hired, new employees are given a copy of the Code of Ethics with a view to a possible placement in at-risk areas, which could require specific training.

Information for external collaborators and *partners*. FATA encourages awareness of and compliance with the Model, also among commercial and financial partners, consultants, various types of collaborators, customers and suppliers, providing specific information on the principles, policies, procedures and texts of the contract clauses that FATA has adopted pursuant to the Model.

6. DISCIPLINARY SYSTEM

6.1 Purpose of the disciplinary system

Setting up a suitable disciplinary system to deal with violations of the regulations contained in the Model or of the provisions and principles of the Code of Ethics **(Attachment 1)** is essential for the Model to be effective and for the Company to be exempt from liability. This disciplinary system aims to prevent the illegal administrative acts related to the crimes indicated in the Decree.

In addition to this, as regards the list of elements to be found in the models prepared by the Entities, art.6, par. 2 *bis*, Legislative Decree 231/2001, letter d) explicitly states that the disciplinary system shall provide for sanctions, even for anyone "*who violates the measures in place to safeguard the whistleblower as well as anyone who with malice or gross negligence makes unfounded reports*".

It is, however, understood that even if a certain type of conduct is not included in the list below, if it is in violation of the Model it could be subject to penalty.

Disciplinary sanctions are applied regardless of the outcome of the criminal action brought by the judicial authority if the conduct to be censured constitutes a crime pursuant to the Decree.

6.2 Measures against employees (non-management)

The disciplinary system establishes the violations to the principles, conduct and specific control elements contained in the Model together with the associated penalties for employees.

All the specific infractions and related sanctions are given in the table below.

Because of its applicability, the Model, including the disciplinary system, shall be officially declared binding for all employees and therefore must be displayed, as specified in art.7, par. 1, Law 300/1970, "*by posting it where it is accessible to everyone*".

The mentioned disciplinary sanctions that are applicable to employees are those included in the current "National collective labor agreement for workers in the private mechanical engineering industry and in the field of plant installation", in compliance with the procedures in art.7 of Law 300/1970 (Workers' statute of rights) and any particular applicable regulations.

It is understood that the disciplinary sanctions applicable to employees will take into account the principle of proportionality as per art. 2106 of the Civil Code, considering in each case the objective seriousness of the event that constitutes a disciplinary offence, the degree of blame, any repetition of the same behavior and the intent of the behavior itself.

For external collaborators, offences could lead to a rescission of contract with or without advance notice.

The above is notwithstanding the right to claim compensation for the damages that occurred as a result of said behavior, including the damages caused by the judge's application of the measures set forth in the Decree.

Two years after their application, disciplinary measures will not be considered for any purpose.

6.3 Measures against Executives

Failure to comply with the Model and violations of the provisions and principles set forth in the Code of Ethics by Executives whose employment is regulated by the current National Collective Employment Agreement for Industry Executives of companies that produce Goods and Services (hereinafter "**C.C.N.L. for Executives**"), will lead to the application of the most appropriate measures (to be imposed by and/or with the support of the Human Resources Department) in compliance with the C.C.N.L. for Executives, including dismissal for the most serious cases, according to the procedures in art.7 of Law 300/1970, notwithstanding the right to claim compensation for damages occurring as a result of said behavior, including damages caused by the judge's application of the measures specified in the Decree.

6.4 Disciplinary System - Summary Table

Non-compliance and conduct by employees that is in violation of the rules set forth in the Model in accordance with the Decree, will entail disciplinary sanctions applied according to the criterion of proportionality in art. 2016 of the civil code, taking into account - with reference to each case - the objective seriousness of the event that constitutes a disciplinary offence, as well as the degree of blame, any repetition of the same behavior and the intent of the behavior itself, as per the table below.

OFFENCES	**NON-EXECUTIVE EMPLOYEES**	**EXECUTIVES**
Substantial non-compliance with the provisions set forth in the "General Principles of Internal Control" with reference to the Control Environment.	Verbal reprimand Written warning Fine not in excess of three hours of basic salary Work and wages suspended up to a maximum of three days Dismissal with advance notice	Suitable measures consistent with CCNL
Non-compliance with the provisions set forth in the "General Principles of Internal Control" with reference to risk assessment, control, information,	Verbal reprimand Written warning Fine not in excess of three	Suitable measures consistent with

reporting and monitoring.	hours of basic salary Work and wages suspended up to a maximum of three days Dismissal with advance notice	CCNL
Failure to observe the conduct specified in the Internal Control System's "Rules of conduct"	Fine not in excess of three hours of basic salary Work and wages suspended up to a maximum of three days Dismissal with advance notice	Suitable measures consistent with CCNL
Failure to comply with the specific elements of the internal control system due to negligence and without exposing the company to an objectively hazardous situation.	Written warning Fine not in excess of three hours of basic salary Work and wages suspended up to a maximum of three days Dismissal with advance notice	Suitable measures consistent with CCNL

Failure to notify the Committee as indicated in the ICS.	Verbal reprimand Written warning Fine not in excess of three hours of basic salary Work and wages suspended up to a maximum of three days Dismissal with advance notice Dismissal without advance notice	Suitable measures consistent with CCNL
At-risk conduct (as listed in the ICS of the operating and instrumental processes) toward public administration officials.	Verbal reprimand Written warning Fine not in excess of three hours of basic salary Work and wages suspended up to a maximum of three days	Suitable measures consistent with CCNL
At-risk conduct (as listed in the ICS of the operating and instrumental processes) which takes the form of an action that also exposes the Company to an objectively hazardous situation.	Work and wages suspended up to a maximum of three days Dismissal with advance notice Dismissal without advance notice	Suitable measures consistent with CCNL

Conduct whose purpose is to unequivocally and intentionally commit a punishable crime under the Decree.	Dismissal with advance notice Dismissal without advance notice	Suitable measures consistent with CCNL
Any other conduct that could potentially lead to the company being subject to the measures indicated in the Decree.	Fine not in excess of three hours of basic salary Work and wages suspended up to a maximum of three days Dismissal with advance notice Dismissal without advance notice	Suitable measures consistent with CCNL
Conduct that entailed the application of the measures in the Decree.	Work and wages suspended up to a maximum of three days Dismissal with advance notice Dismissal without advance notice	Suitable measures consistent with CCNL
Gross negligence in making a report as per art. 6 par. 2 *bis* of Decree Law 231/2001, which proves to be unfounded	Work and wages suspended up to a maximum of three days	Suitable measures consistent with CCNL
Intentionally making a report as per art. 6 par. 2 *bis* of Decree Law 231/2001, which proves to be unfounded	Dismissal with advance notice Dismissal without advance notice	Suitable measures consistent with CCNL
Gross negligence in violating whistleblower safeguards	Work and wages suspended up to a maximum of three days	Suitable measures consistent with CCNL
Intentional violation of whistleblower safeguards	Dismissal without advance notice	Suitable measures consistent with CCNL

6.5 Measures against self-employed individuals/collaborators

Failure to comply with the rules of the Model as well as violations of the provisions and principles established in the Code of Ethics and in art. 6 par. 2 *bis* of Legislative Decree 231/2001 concerning reporting and the right to confidentiality, by each self-employed individual/collaborator, could lead to the rescission of the contract in accordance with the provisions of the employment contract, notwithstanding

the right to claim compensation for damages occurring as a result of said behavior, including the damages caused by the judge's application of the measures in the Decree.

6.6 Measures applicable to subjects who have contractual/commercial relations with FATA

Failure to comply with the rules of the Model as well as violations of the provisions and principles established in the Code of Ethics and in art. 6 par. 2 *bis* of Legislative Decree 231/2001 concerning reporting and the right to confidentiality, by subjects who have contractual / commercial relations with FATA, could lead to the rescission of the contract in accordance with the provisions of the employment contract, notwithstanding the right to claim compensation for damages occurring as a result of said behavior, including the damages caused by the judge's application of the measures in the Decree.

6.7 Measures against Directors

In the case of violation by the Directors of the Model and of art. 6 par. 2 *bis* of Legislative Decree 231/2001 concerning reporting and the right to confidentiality, the Committee shall inform the company's Board of Statutory Auditors, which shall take the necessary initiatives specified in current regulations.

6.8 Measures against Statutory Auditors

In the case of violation by one or more Statutory Auditors of the Model and of art. 6 par. 2 *bis* of Legislative Decree 231/2001 concerning reporting and the right to confidentiality, the Committee shall inform the Board of Directors, which shall take the most appropriate initiatives.

6.9 Measures against members of the Supervisory Committee

If the Board of Directors is informed of violations by one or more members of the Supervisory Committee of this Model and of art. 6 par. 2 *bis* of Legislative Decree 231/2001 concerning reporting and the right to confidentiality, it shall take the most appropriate initiatives.

6.10 Subjects authorized to apply disciplinary measures

The disciplinary system is subject to constant verification and evaluation by the Committee and the Department of Human Resources, responsible for actually applying the outlined disciplinary measures, possibly on the recommendation of the Committee and after having heard the superior of the person who engaged in censurable conduct.

7. MODEL AND CODE OF ETHICS

The rules of conduct described in the Model are integrated with those of the Code of Ethics even though the scope of the Model differs from that of the Code in terms of the purposes it intends to pursue to implement the provisions of the Decree.

In this respect, in fact:

- the Code of Ethics is an independently adopted instrument and could be applied in general by the Company for the purpose of expressing principles of "company ethics" that FATA acknowledges as its own and demands that all company representatives comply with;
- the Model, on the other hand, fulfils the specific requirements contained in the Decree, which aim to prevent particular types of crimes from being committed (due to events which appear to have been committed for the benefit of the Company but which could entail administrative liability based on the provisions of the Decree itself).

8. VERIFYING THE APPLICATION AND SUITABILITY OF THE MODEL

The Model is subject to the following types of checks:

- Monitoring the effectiveness of the Model (which actually verifies the consistency between the types of conduct by Model recipients) by setting up a system where periodical declarations are made by the managers of corporate areas which come into contact with the Public Administration (see the Evidence Sheets in **Attachment 4**). This system can confirm that:
  - sufficient evidence has been provided regarding transactions carried out with the Public Administration in the areas at risk of a crime being committed;
  - the indications and content of the Model, proxies, delegation of powers and signatory limits have been fulfilled, and no infractions or actions have been undertaken that are not in line with the Model.

  The managers of at-risk areas are responsible for having their subordinates fill out the declarations and for submitting them to the Committee, which will file and check them at random.

- Verification of procedures: the Model's actual operation is checked on a yearly basis in the manner established by the Committee. All the reports received throughout the year are periodically *reviewed*, as are the actions carried out by the Committee and by the other stakeholders, the events considered to be at risk and the personnel's awareness of the types of offences set forth in the Decree, by means of random checks. The outcome of this review, which highlights any shortcomings and suggests which actions should be undertaken, is included in the periodical report prepared by the Committee for the company's Board of Directors.

The Committee determines which changes to the Model should be submitted to FATA's Board of Directors for approval.

The Committee is also responsible for:

- issuing and updating standard instructions for the managers of at-risk areas on how to fill out the Evidence Sheet in a uniform and consistent manner. These instructions shall be written and kept on paper or electronic media;
- periodically checking - with the assistance of the other authorized departments - the current power delegation system, while recommending changes if the powers of directors and/or their qualifications do not match the powers of representation conferred on the internal officer or deputy officers, and the validity of the required standard clauses whose purpose is to:
  - ensure that external collaborators and partners comply with the Model and the Code of Ethics;
  - enable FATA to effectively run checks on the recipients of the Model in order to make sure that its provisions are being complied with;
  - implement sanctioning mechanisms (in the case of withdrawal from contract by *partners* or external collaborators, for example) if requirements are not fulfilled.

SPECIAL SECTION "A"

Areas of business in which crimes could be committed to the detriment of the Public Administration, pursuant to articles 24 and 25, bribery among private individuals pursuant to art. 25-ter lett s-bis) and art. 25-*quinquiesdecies*

1. PURPOSE

This Special Section refers to conduct by FATA employees, boards and consultants involved in Sensitive Processes.

The aim of this Special Section is to have all the recipients adopt the rules of conduct described herein in order to prevent the crimes listed herein from being committed.

2. SENSITIVE PROCESSES

The business areas in which the crimes in the Decree could be committed concern relations with the Public Administration (hereinafter **PA**), and the situations in which it is involved (crimes against the PA and property crimes, pursuant to articles 24 and 25 of the Decree), and the crime of bribery among private individuals, as governed by art. 25 *ter* lett s-bis), as well as tax crimes (as per art. 25 *quinquiesdecies*).

Considering the particular nature of FATA's business and internal organization, in order to set up a risk management system that is consistent with the Decree's requirements, the following two categories of areas have been tentatively identified for analysis:

- AREAS AT RISK OF CRIME - OPERATING PROCESSES: areas where, based on information collected and shared with area managers, there are relations with the PA, meaning that the crimes in articles 24 and 25 *ter* lett s-*bis),* 25 *quinquiesdecies,* could potentially be committed;
- SUPPORT AREAS - INSTRUMENTAL PROCESSES: areas in which financial instruments (and/or replacements) are handled, where, even if there are no relations with the PA, there could be encouragement to commit crimes in the areas at risk of crime.

The areas, divided as above, are:

OPERATING PROCESSES

- Authorizations, concessions and relations with control institutes and bodies
- Sales.

INSTRUMENTAL PROCESSES

- Selection and management of personnel;
- Operative finance and cash management;
- Gifts, hospitality and entertainment expenses;
- Professional consulting and services;
- Sponsorships, advertising campaigns and contributions
- Settlement agreement;
- Purchase of goods and services.

The processes described above, which are at risk of crimes being committed as described, analyzed in the following sheets, may also give rise to the same types of crimes committed by criminal organizations. It follows that the prevention and control protocols indicated in the mentioned sheets are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

Likewise, the control protocols indicated in the sheets - in addition to the specific general principles in Special Section E - are also a way to prevent crimes of money laundering and use of illegal money, to which some of the above-mentioned processes are exposed.

For the purpose of specifically identifying said processes, in the sheets, the paragraph "Criminal Conspiracy" also includes the crimes of money laundering, use of illegal money and bribery among private individuals, which are still not classifiable as crimes under this Special Section.

3. RECIPIENTS

The Recipients of this Special Section are the Directors, Executives and Employees operating in at-risk business areas, and all the external collaborators and *Partners* (all referred to as "**Recipients**"). The aim of this Special Section is to ensure that all the recipients are aware of the significance of censurable conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

4. OPERATING PROCESSES

4.1 Authorizations, concessions and relations with control institutes and bodies

ACTIVITIES

The processes concerning authorizations and concessions refer to activities performed for the purpose of obtaining (and subsequently dealing with the PA):

- space for offices or plants (i.e. excavations on public grounds or toll highways), advertising material, rights to use information (such as traffic information) and sponsorships, by stipulating sale agreements and contracts and leases;
- administrative measures for activities related to real estate used for operations and plants (i.e. offices and industrial facilities).

The processes for dealing with the control institutes and bodies refer to:

- disclosure / reporting obligations with respect to independent authorities / supervisory and control bodies (i.e. Data Protection Authority, CONSOB, etc.);
- periodical obligations of statutory, fiscal and accident prevention regulations, etc.

These processes are essentially similar and divided into the following phases:

- contact with public officials to explain what is required;
- submitting the request, and, if necessary, negotiating technical and design specifications and contractual clauses;
- release of authorization or stipulation of the contract;
- handling relations during the period of validity of the authorization or contract, with final check and/or test;
- handling inspections/investigations and/or any legal action.

RELATED CRIMES

In regard to these processes, the possible crimes could tentatively be: **bribery and fraud to the detriment of the State, of a public entity or of the European Union, or to receive public funds, computer fraud to the detriment of the State or of a public entity.**

The crime of bribery could be committed to obtain an authorization, stipulate a contract or influence the outcome of an inspection.

The crime of fraud to the detriment of the State or of the European Union, or to receive public funds could take the form of an untrue document or misleading conduct that is financially damaging to the State, the EU or a public entity (e.g. in unit-price excavation agreements, where the amount of work declared is less than what was actually carried out, for the purpose of paying a smaller amount).

CONTROL ACTIVITIES

The control system is based on the key element of **document traceability**.

The specific control elements are listed below:

- a check to verify that what was authorized is consistent with what was performed and what was declared to the Public Administration for the purpose of paying the required fees;
- traceability of the documents and sources of information during each phase of the processes with specific reference to the use of resources and time;
- for each operation or several operations if they recur - of the people delegated to deal with the Public Administration;
- directives regarding the type of conduct to adopt in formal and informal dealings with various public officials;
- formalization of relations with external individuals (consultants, third-party representative or other) who perform activities for FATA, including in the contracts a specific clause binding them to the principles of ethics and conduct adopted by the Company;
- selection and use of suppliers from the Register of Qualified Suppliers and instructions on how to determine a *vendor rating*, including for any external professionals whose services are used by the company.

Moreover, suitable *escalation* procedures must be established to deal with any exceptions to the above-mentioned principles.

INSTRUCTIONS ON CONDUCT

Do not adopt types of conduct that carry the risk of a crime being committed and/or that are contrary to the Code of Ethics, in all process phases, and particularly in the following activities:

- while preparing and presenting the necessary documentation, if said conduct is aimed at influencing the stipulation of the contract or the release of an authorization;
- during inspections/investigations by the PA, if said conduct is aimed at influencing the judgement/opinion of the public representatives.

INFORMATION FLOWS TO THE SUPERVISORY BODY

The department heads concerned with authorizations issued by the PA, stipulating concession contracts and signing agreements, shall provide, at given intervals, the following flows of information which concern them:

Flow 1: list of measures obtained and contracts stipulated;

Flow 2: list of disputes and legal actions brought by the PA

4.2 Sales

ACTIVITIES

This process refers to the activities carried out in connection with the supply of goods and services for public officials based on contracts stipulated following a public procurement procedure.

The process is divided into the following stages:

- acquisition of information concerning the public procurement procedure, or contact with the public official in the case of negotiated procedures;
- preparation of the offer and participation in the public procurement procedure, or dealing with the public official in the case of private negotiations;
- stipulation and performance of the contract and testing/verification;
- invoicing, credit management, payments and any objections.

RELATED CRIMES

In regard to these processes, the possible crimes could tentatively be: **bribery, fraud to the detriment of the State, to the EU or to a public entity, fraud in public procurement, computer fraud, money laundering and use of illegal capital.**

The crime of **bribery, even among private individuals**, could be committed, for example, to have a contract awarded or to influence the outcome of a test.

The crime of **fraud to the detriment of the State, to the EU or to a public entity** could take the form of an untrue document or misleading conduct for the purpose of damaging the property of the State.

The crime of **money laundering** could be committed following a failure to first verify the reliability of the commercial counterparts and/or operating/financial partners before stipulating agreements (ATI/RTI) with other companies to carry out the activities.

The crime of **computer fraud** could be committed by changing the operation of systems or acting on data in order to obtain unfair advantages for the Company.

CONTROL ACTIVITIES

The control system is based on the fundamental elements of role separation in the key process phases and on document traceability.

In particular, the specific control elements are listed below.

- Existence of different players operating in the following phases/activities of the processes:
  - preparing the offers for the bidding process, negotiated definition of specifications or running the negotiations
  - managing the supplier register for sub-supplies;
  - contract performance;
  - invoicing.

- Signing of a specific document by the person in charge of the offer, declaring compliance with the principles of ethics and conduct adopted by the Company, to be attached to the tender documents/private negotiations with the PA.
- A check to verify consistency between what was contracted, tested/certified and invoiced to the Public Administration.
- Traceability of the documents and sources of information during each phase of the process with specific reference to the use of resources and time.
- Verifying the reliability of commercial counterparts.
- Identifying the selection criteria for partners on agreements/joint ventures and in temporary joint ventures (ATI/RTI) with other companies to carry out the activity.
- Establishing the minimum requirements of bidders on temporary joint ventures (ATI/RTI) and setting the criteria to evaluate the offers on standard contracts.

Moreover, suitable escalation procedures must be established to deal with any exceptions to the above-mentioned principles.

INSTRUCTIONS ON CONDUCT

Do not adopt types of conduct that carry the risk of a crime being committed and/or that are contrary to the Code of Ethics, in all process phases, and particularly in the following activities:

- Preparing and sending tender documentation:
  - while collecting/drawing up technical-administrative documentation, if the conduct is such that it intends to show the PA information that is untrue and/or incomplete or to circumvent legal obligations;
  - while checking compliance with the requirements of the invitation to tender and identifying the winning bidder, if the purpose of the conduct (i.e. the sales departments undertake to select without motive, sub-suppliers who are to the "liking" of the PA representatives) is to persuade the above-mentioned representatives to prefer the Company's position.

- While making any changes or additions to the contract, if the purpose of the conduct is to persuade the PA representatives to prefer the Company's position.
- During inspections/investigations by the PA, if said conduct is aimed at influencing the opinion of the inspectors/investigators.
- While dealing with any disputes with the PA, if the purpose of the conduct is to circumvent legal obligations and advance the interests of the company.

– During negotiations with counterparts that do not belong to the PA, if a conduct is adopted that aims to influence the evaluation of the company's position.

INFORMATION FLOWS TO THE SUPERVISORY BODY

The head of the Sales Department shall provide the following information at given intervals:

Flow 1: list of stipulated contracts/sales orders for goods/services whose value is above the threshold (together with a list of contract changes greater than 10%);

Flow 2: list of sales contracts with intermediation.

5. INSTRUMENTAL PROCESSES

5.1 Selection and management of personnel

ACTIVITIES

The personnel selection and management process includes all the activities needed to create a work relationship between the Company and a natural person. The process is created for all the professional segments concerned (managers, qualified professionals, recent university and high school graduates) and essentially comprises the following phases:

– receipt and management of resumés (hereinafter "CV");
– selection;
– preparation of the offer and hiring;
– management of employees' personal data.

CRIMES

The selection and hiring process constitutes one of the instrumental means through which the crime of **bribery - including among private individuals - and tax crimes** could in principle be committed.

The selection and hiring of personnel could in fact constitute a possible aid to committing a crime against third parties, public officials or public service officers to obtain favors in the performance of other company activities (i.e. sales, obtaining licenses or authorizations from the PA, etc.).

An illicit benefit obtained by hiring personnel is what constitutes the aforementioned crime, together with the position of the third party, public official or public service officer of the victim and the official actions to be performed, omitted or delayed.

Moreover, this phase also includes the crime of employing third-country citizens without a valid residence permit even if this does not fall within the crimes considered in this Special Section as it pertains to the instrumental process in question.

CONTROL ACTIVITIES

The control system is based on the key elements of **role separation** between the HR department and the departments that use the resources, and of **traceable evaluation situations**.

In particular, the specific control elements are listed below.

- in the phase "CV acquisition and management", traceability of the CV sources (e.g. *head-hunting companies*, *e-recruitment*, announcements, voluntary applications, internal presentations, etc.);
- in the phase "Selection", fulfillment of the criterion of organizational separation for candidate evaluation. For this purpose:
  - establish different means for the "aptitudinal" and "technical" evaluation of candidates;
  - assign the responsibility for these evaluations to different individuals;
  - request that the individuals performing these evaluations formally sign them to ensure traceability of the choices that are made;

- in the phase "Preparation of the offer and hiring":
  - make the selection after having assessed the candidate's fitness;
  - check the candidate's personal documentation, especially as regards candidates from non-EU countries, ensuring that they have a valid residence permit, and when the letter of employment is signed, check that documentation is attached proving that the previous phases were carried out properly.

- in the phase "Preparation of the offer and hiring":
  - perform periodical checks to ensure that the personnel file matches the actual workforce.

This process must also include formal *escalation* procedures to deal with any exceptions to the above-mentioned principles. As regards the signing of the employment letter, *escalation* makes it possible for individuals to appeal to someone who holds a higher position (hierarchical or operational) than the person who signed the letter.

INFORMATION FLOWS TO THE SUPERVISORY BODY

The HR department shall regularly provide the following information, insofar as it concerns said department:

Flow 1: list of hires that deviate from the above-mentioned principles and/or because of internal reports.

5.2 Operative finance and cash management

ACTIVITIES

The process refers to activities concerning outgoing monetary and financial flows for the purpose of fulfilling various obligations of the Company's business units.

The above-mentioned flows are basically divided into two macro groups:

- ordinary flows connected with current activities/operations (i.e. purchase of goods, services and licenses, financial, fiscal and social security charges, wages and salaries);

- extraordinary flows connected with financial transactions (i.e. subscription and increase of share capital, loans to group companies, credit transfers, foreign exchange transactions and transactions involving derivatives - *swaps*, *futures*, etc.).

The process is divided into the following stages:

- planning of periodical and/or spot financial requirements, and duly authorized disclosure to the financial department in question;
- preparation (by the latter) of financial resources, on the required dates and at the required banks;
- requesting an order for payment or to make the resources available;
- end use of the sum in accordance with the instructions of the Company.

RELATED CRIMES

The cash and financial management process constitutes one of the instrumental means through which the crimes of **bribery - including among private individuals - money laundering and use of illegal capital** could in principle be committed, **in cases of conduct damaging to the financial interests of the European Union.** This process could in fact constitute assistance in establishing financial resources - both in Italy and abroad - intended for public officials or public service officers.

CONTROL ACTIVITIES

The control system is based on the main elements of **formal role separation** in the key process phases, on the **traceability of documents** and **levels of authorization** to be associated to the transactions.

In particular, the specific control elements are listed below.

- Existence of different players operating in the following phases/activities of the process:
  - Requesting an order for payment or provision of funds;
  - Making the payment;
  - Performing checks/reconciliation of actual transactions.

- Existence of authorization levels for both payment requests and orders and provision of funds, depending on the type of transaction (ordinary/extraordinary) and the amount.
- Existence of a systematic flow of information that ensures constant alignment between powers of attorney, operating powers and authorization profiles residing in the IT systems.
- Existence and divulging of signature samples of the authorization levels established for the request.
- Performing periodical reconciliations of both intercompany accounts and bank accounts.
- Traceability of the documents and of each phase of the process (with specific reference to the cancellation of documents that have already generated a payment).
- Checking the reliability of financial partners on extraordinary financial transactions (i.e. subscription and increase of share capital, financing, credit transfers, foreign exchange transactions, etc.).
- Existence of formal substantial checks of corporate financial flows with reference to payments to third parties and payments/transactions among group companies.
- Checking of cash flow (to ensure it does not exceed the threshold for cash payments, possible use of a bearer or anonymous passbook to manage liquidity, etc.).
- Checking that financial transactions are legitimate and that recipients/ordering parties match the counterparts that are actually involved in the transactions.

- Checking that book keeping is being done correctly

- Checking the economic or corporate context to determine the extent and type of tax risk
- Checking that the declarations have been properly filed
- Checking the tax and VAT returns, to be done by someone other than the individual who prepared the declarations

Any non-standard procedures (for both ordinary and extraordinary transactions) must be considered "exceptions" and therefore subject to the following specific authorization and control criteria:

- identification of the individual that can request the transaction;
- identification of the individual that can authorize the transaction;
- indication of the reason by the applicant;
- appointment (if necessary) of a resource authorized to make / authorize the transaction through an ad hoc power of attorney.

INFORMATION FLOWS TO THE SUPERVISORY BODY

The head of Administration, Finance and Control must provide the following information at given intervals, insofar as it concerns him/her:

Flow 1: Deviations from the financial *budget* that exceed the threshold and are not justified by the performance of the *business*.

Flow 2: list of non-*standard* monetary and/or financial flows (extraordinary transactions) that occurred in the period.

5.3 Gifts, hospitality and entertainment expenses

For public employees and directors

ACTIVITIES

The process of gift giving, hospitality and entertainment expenses comprises all the activities required to provide goods and services free of charge and to bear the above-mentioned expenses, regardless of whether or not they come under the company's actual business activities, to customers, suppliers, sales teams, employees and individuals outside the company for the purpose of developing the company's sales activity, directly encouraging demand for the company's goods and services and indirectly promoting it.

The process is divided into the following stages:

- Planning and divulging requirements in terms of gifts, hospitality and entertainment expenses;
- Requesting and authorizing gifts, hospitality and entertainment expenses
- Identifying the supplier of the gifts and their subsequent purchase;
- Bearing the expenses and performing the checks;
- Handling the provision of goods /services (directly and through the warehouse).

RELATED CRIMES

The process of gift giving, entertainment expenses and hospitality constitutes one of the instrumental means through which the crime of **bribery - including among private individuals - and tax crimes** could in principle be committed.

Irregular handling of gift giving, entertainment expenses and hospitality could in fact constitute a possible aid to committing a crime against third parties, public employees and directors in order to obtain favors in the performance of other company activities (i.e. sales, obtaining licenses or authorizations from the PA, etc.).

An element of the crime of bribery, in addition to the position of the third party, public official or public service officer, is the illegal receipt by the latter of remuneration or any other benefit for him or herself or for third parties, resulting from the performance, omission or postponement of a required official act.

CONTROL ACTIVITIES

The control system is based on the fundamental elements of **role separation between the applicant and the recipient** of the gift, entertainment expenses and hospitality, and on the **specific limits placed on the monetary value** of gifts, entertainment expenses and hospitality intended for third parties, public employees and directors.

In particular, the specific control elements are listed below.

- Identification of corporate individuals who are authorized to:
  - give gifts, request entertainment expenses or hospitality (applicant);
  - determine the recipients of entertainment expenses or hospitality;
  - authorize requests;
  - supply gifts (recipient).

- Existence, for each type of good/service, of specific price ranges (and the corresponding maximum amount that can be spent).
- Existence of a "catalogue" of the types of goods/services that can be given as gifts (agendas, calendars, corporate gadgets, subscriptions, etc.).
- Existence of limits on entertainment expenses and hospitality
- Registration of gifts given to third parties, public employees and directors, by the company individual who made the request.
- Documentary evidence of each process phase (request, purchase, identification and delivery/issue) provided by the involved individuals.
- Checking that receipts, invoices and equivalent documents are properly registered in accordance with tax legislation.

Also required are *escalation* procedures to manage powers (especially if the maximum amount is exceeded), with the necessary opinion of the legal department.

INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The head of the Purchasing and Logistics Department and Top Management Figures shall regularly provide the following information, insofar as it concerns said department:

Flow 1: list of gifts handed out and entertainment and hospitality expenses incurred in connection with third parties, public employees and directors, that exceed the limit.

5.4 Consulting

ACTIVITIES

This regards the assignment of consulting and professional services to third parties, and in spite of the specific nature of the subject of the contract, is therefore considered to be a procurement process divided into the following phases:

- Establishing a budget and plan for a given period;
- Issuing the request for consulting/professional services;
- Selecting the supplier and stipulating a contract;
- Managing the contract;
- Issuing approval for, calculating and paying invoices.

RELATED CRIMES

The process of assigning professional consulting/services constitutes one of the instrumental means through which the crime of **bribery - including among private individuals - and tax crimes** could in principle be committed.

The crime of bribery could be committed through non-transparent assignments (i.e. by creating funds in connection with services contracted at higher than market prices, or through assignments to people or companies who are agreeable to third parties or public individuals, for the purpose of obtaining favors in connection with the performance of other company activities).

An illicit benefit obtained by hiring personnel is the element constituting the aforementioned crime, together with the position of the third party, public official or public service officer of the victim and the official actions to be performed, omitted or delayed.

CONTROL ACTIVITIES

The control system is based on the two main elements of formal role separation in the key process phases and on document traceability to guarantee transparency of the choices made and the service received.

In particular, the specific control elements are listed below.

- Existence of different players operating in the following phases/activities of the process:
  - request for consulting/service;
  - authorization;
  - contract stipulation;
  - certificate of services performed (consent issued);
  - payment.

- Existence of the professional, economic and organizational requirements needed to guarantee the required quality standards (supplier register) and of complete assessment mechanisms of the service rendered (*Vendor Rating*).
- A suitable process of selection among various bidders with an objective comparison of offers (based on objective, documented criteria).
- Use of suitably formalized contractual mechanisms.
- For professional consulting/services performed by third parties assigned to represent FATA in dealing with third parties, including the PA, a specific clause has to be drawn up which obligates them to comply with the principles of ethics and conduct adopted by the Company.
- Existence of levels of approval for requests of consulting/services and for certification/validation of the services rendered, as well as transparent authorization levels (consistent with the company's system of powers) for the stipulation of contracts and the approval of any variations/additions.

- Traceability of each process phase (supporting documents, level of formalization and archiving procedures/time), in order to recreate the responsibilities, reasons for choices and information sources.
- Checking that invoices and expense statements submitted by consultants in connection with their mandate/contract and the professional services rendered are correct.

Moreover, suitable operating procedures together with the corresponding escalation mechanisms must be established to deal with any exceptions to the above-mentioned principles, whenever necessary, for requirements of confidentiality and promptness, for example.

INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The Company's top management shall report the following at set intervals:

Flow 1: All the assignments, with the exception of operating/technical ones connected with job management; all those lasting more than one year.

5.5 Sponsorships

ACTIVITIES

The process concerns expenses incurred for third parties to promote the Company's image.

The process is divided into the following stages:

- establishing a budget and plan for a given period;
- identifying sponsorship initiatives and potential partners;
- negotiating and stipulating a contract of commitment;
- managing the contract;
- issuing the approval, calculating and paying invoices.

RELATED CRIMES

The sponsorships constitute one of the instrumental means through which the crime of **bribery - including among private individuals - and tax crimes** could in principle be committed.

Irregular handling of sponsorships could constitute a possible aid to committing a crime against third parties, including public employees and directors, to obtain favors in the performance of other company activities (i.e. sales, obtaining licenses or authorizations from the PA, etc.).

CONTROL ACTIVITIES

The control system is based on the fundamental elements of determining the criteria to identify sponsorship projects and of a suitable contract structure.

The specific control elements are listed below:

- Creating and formally distributing a company policy to carry out sponsorship projects (criteria to identify the areas - social, cultural, sports, etc. - of the initiative and the requirements of the partners).
- Use of suitably formalized contractual mechanisms subject to professional validation by the Legal Department, as well as transparent authorization levels (consistent with the company's system of powers) for the stipulation of contracts and the approval of any variations/additions.

- Existence of different players operating in the various phases/activities of the process (approval of the annual program of sponsorship projects, stipulation of contracts, payments).
- Formalization of relations with external individuals (consultants, third-party representatives or other) who perform activities for the Company, whose contracts include a specific clause that binds them to the principles of ethics and conduct adopted by the Company.
- Traceability of each process phase in order to recreate the responsibilities, reasons for choices and information sources.
- Checking that receipts, invoices and equivalent documents are properly registered in accordance with tax legislation.

Moreover, suitable escalation procedures must be established to deal with any exceptions to the above-mentioned principles.

INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The Company's top management shall report the following at set intervals:

Flow 1: Immediate report on sponsorship projects for amounts that exceed the threshold or with the PA;

Flow 2: List of initiatives taken on by the company.

5.6 Settlement Agreements

ACTIVITIES

This process concerns all the activities needed to prevent or settle a dispute with third parties; the particular aim of these activities is to come to an agreement with third parties by making mutual concessions, thus avoiding judicial proceedings.

Disputes may derive from a contractual relationship or from non-contractual liabilities (i.e. if a dispute occurs because of damage to the Company caused by third parties and vice-versa).

The process is divided into the following stages:

- analysis of the event that led to the dispute;
- determining if the necessary conditions exist in order to reach a settlement;
- activities to determine and formalize the settlement;
- drawing up, stipulating and executing the settlement agreement.

RELATED CRIMES

The settlement agreement process constitutes one of the instrumental means through which the crime of **bribery - including among private individuals - and tax crimes** could in principle be committed.

The irregular handling of the settlement process could in fact constitute a potential way to arrange the financial means needed to guarantee the "funds" including for the purpose of committing the major crimes described in the Decree.

CONTROL ACTIVITIES

The control system is based on the fundamental elements of **role separation** between the key process phases and on **phase traceability** to guarantee the choices that form the basis of the settlement agreement.

In particular, the specific control elements are listed below.

- Existence of different responsibilities such as:
  - Managing the company process connected with the settlement agreement;
  - Managing the negotiations and formalization of the settlement agreement.

- Existence of documentary evidence of each process phase (request, purchase, identification and execution of the agreement) provided by the individuals involved.
- Existence of authorization levels consistent with the company's systems of powers to stipulate and execute settlement agreements.
- Existence of the quality/quantity criteria needed to use settlement agreements as an alternative to dealing with the dispute in a court of law.
- Checking the amount stated in the settlement agreement, to be done by a competent individual other than the person who reached an amicable settlement of the dispute;

Also required are *escalation* procedures to manage the powers (especially if the maximum amount is exceeded), and the mandatory opinion of the legal department.

INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The company's top management shall regularly provide the following information, insofar as it falls within its responsibilities:

Flow 1: list of settlements, specifically highlighting those dealt with as exceptions.

5.7 Purchase of Goods and Services

ACTIVITIES

The process is divided into the following stages:

- planning of needs and budget and establishing a purchase plan;
- issuing the purchase request;
- selecting the supplier and stipulating a contract;
- managing the contract/order (rendering of services/delivery of goods);
- issuing the approval, calculating and paying invoices.

CRIMES

The procurement of goods and services constitutes one of the instrumental means through which the crime of **bribery - including among private individuals, money laundering and the use of illegal capital, as well as tax crimes** could in principle be committed.

The crime of **bribery** could be committed through a non-transparent procurement process (i.e. by creating funds in connection with contracts stipulated at higher than market prices, or by awarding contracts to people or companies who are agreeable to public individuals for the purpose of obtaining favors in connection with the performance of other company activities).

An illicit benefit obtained through the procurement process is the element constituting the aforementioned crime, together with the position of the third party, public official or public service officer of the victim and the official actions to be performed, omitted or delayed.

The crime of **money laundering** could be committed following a failure to first verify the reliability of the commercial counterparts and/or operating/financial partners before stipulating agreements (ATI/RTI) with other companies to carry out the activities.

Tax crimes could be committed following a failure to perform a preliminary check on the proper keeping of accounts.

CONTROL ACTIVITIES

The control system is based on the fundamental elements of **formal role separation** in the key process phases, on **document traceability** and on **full evaluation of the supplied items**.

In particular, the specific control elements are listed below.

- Existence of different players operating in the following phases/activities of the process:
  - requesting the supply;
  - selecting the supplier;
  - making the purchase;
  - certifying the services performed/goods delivered (consent issued);
  - payment.

- Existence of technical-economic criteria for:
  - the selection of potential suppliers (suppliers' reliability and qualification must be verified and they must be entered in a Supplier Register, possess the necessary commercial and professional requirements, and verification of financial flows);
  - validation of the supply and of the supplied goods/services (Incoming Quality);
  - complete evaluation of suppliers (*Vendor Rating*).

- A suitable process of selection among various bidders with an objective comparison of offers (based on objective, documented criteria).
- Use of suitably formalized contractual mechanisms.
- Existence of levels of approval for purchase requests and for certification of the services rendered, as well as authorization levels (consistent with the company's system of powers) for the stipulation of contracts and the approval of any variations/additions.
- Traceability of each process phase (supporting documents, level of formalization and archiving procedures/time), in order to recreate the responsibilities, reasons for choices and information sources;
- Traceability of checks performed to ensure the service/supply was properly rendered and making sure the order and the invoice match

Moreover, suitable *escalation* procedures must be established to deal with any procurement activities that deviate from the above-mentioned principles (i.e. selection of suppliers that are not on the register, failure to compare alternative offers, etc.)

INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The head of the Procurement and Logistics Department shall regularly provide the following information, insofar as it concerns said department:

Flow 1: list of purchases that exceed the limit;

Flow 1: list of purchases that deviate from the above-mentioned requirements;

SPECIAL SECTION "B"

Areas of business in which corporate crimes could be committed, pursuant to articles 25 *ter* and 25 *sexies* of Legislative Decree 231/2001

1. PURPOSE

This Special Section refers to conduct by FATA employees, boards and consultants involved in sensitive processes.

The aim of this Special Section is to have all the above-mentioned recipients adopt the rules of conduct described herein, in order to prevent the crimes listed herein from being committed.

2. SENSITIVE PROCESSES

The principal sensitive processes identified by FATA within its organization are:

- reporting to the shareholder on the income, assets and liabilities and financial position of the Company (Annual Report), plans, *budgets* and prospectuses, in the case of extraordinary and particular transactions;
- managing and divulging news/data outside the Company (relations with institutional investors, *price-sensitive* announcements);
- operations involving share capital;
- periodical reporting to financial markets;
- transactions on own financial instruments, negotiating derivatives and plans for the purchase of treasury shares.
- All the operating and instrumental processes specified in Section A that constitute a crime of bribery among private individuals.

The processes described above, which are exposed to the risk of corporate crimes being committed as described in this Special Section, may also give rise to the same types of crimes committed by criminal organizations. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

3. RECIPIENTS

The Recipients of this Special Section are the Directors, General Managers (top management figures) and Statutory Auditors of FATA, as well as employees subject to surveillance and control by top management figures in at-risk business areas, hereinafter referred to as "**Recipients**".

As regards the Directors, General Directors and Statutory Auditors, the law equates those who perform these duties "de facto" with those who are formally vested with these titles. Pursuant to art. 2639 of the civil code, in fact, anyone who performs the same job that is described differently, as well as anyone who continuously exercises the typical powers of the title or job, must answer for the corporate crimes found in the Civil Code.

The aim of this Special Section is to ensure that all the Recipients are fully aware of the significance of censurable conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

4. GENERAL RULES OF CONDUCT

This Special Section states that the "Recipients" are specifically prohibited from:

- engaging in, collaborating with or giving rise to conduct that could come under the types of crimes considered (art. 25-*ter* and 25-*sexies* of the Decree);
- engaging in, collaborating with or giving rise to conduct that, even if it does not actually constitute one of the crimes considered (art. 25-ter and 25-sexies of the Decree), could potentially become one;
- violating the principles and procedures of the company as specified in this Special Section.

This Special Section consequently states that the above-mentioned Recipients are specifically obligated to:

1. Conduct themselves in a fair, transparent and collaborative manner in compliance with the law and the company's internal procedures, in all activities aimed at preparing the annual report and other corporate reports, for the purpose of providing the shareholder and third parties with true and correct information concerning the income statement, assets and liabilities statement and financial position of the Company. In particular, they are prohibited from:

- showing or transmitting, for the purpose of processing and entering in the annual report, reports and schedules or other corporate reports, false or incomplete data or data that does not reflect the real situation of income, assets and liabilities and financial position of the Company;
- omitting data or information required by law regarding the income, assets and liabilities and financial position of the Company.

2. Rigorously comply with all the legal requirements that safeguard the integrity and effectiveness of the share capital so as not to harm the guarantees of creditors and third parties in general. They are particularly prohibited from acting in a manner that would make the company boards adopt one or more of the following behaviors or actions:

- return contributions to the shareholders or release them from the obligation of making them, with the exception of cases of legitimate reduction in share capital;
- distribute profits or advance payments on profits that have not actually been received or that are earmarked by law as reserves;
- purchase or subscribe shares of the Company or of controlled companies in cases not provided for by law, thus damaging the integrity of the share capital;
- perform reductions in share capital, mergers or spin-offs in violation of the provisions of the law that safeguard creditors, causing them harm;
- fictitiously create or increase share capital, assigning shares a value lower than their face value when increasing share capital;
- in the liquidation of a company, divert corporate assets intended for creditors, distributing them among the shareholders before paying the creditors or setting aside the amounts needed to pay them.

3. Ensure that the Company and its boards are running smoothly, guaranteeing and facilitating any type of internal control on corporate operations required by law, as well as allowing the shareholders to freely express their will. In particular, they are prohibited from:

- engaging in conduct that materially prevents, by concealing documents or using other fraudulent means, or that could somehow hinder inspections and audits by the shareholders, the Board of Statutory Auditors or the auditing company;

- determining or influencing the deliberations of the shareholders' assembly, by means of simulated or fraudulent actions aimed at altering the decision-making process of the assembly.

4. Conduct themselves in a manner that is inappropriate for doing business with third parties or Public Administration employees as identified in the sensitive areas described in "Special Section A".

5. DOCUMENTS DISTRIBUTED TO THE COMPANY BOARDS OF FATA

In performing all the corporate management operations, in addition to the rules included in this Model, FATA's boards must generally know and comply with:

- FATA's Code of Ethics;
- the internal control system as well as the directives of the Parent Company, company procedures and management control system;
- the documentation and provisions relating to the company's operational-hierarchical and organizational structure (organization charts);
- the company's manual of procedures (if it exists);
- the disciplinary system described in the National Collective Employment Agreement (CCNL) and in the National Collective Employment Agreement for Industry Executives;
- in general, the applicable Italian laws.

6. TYPES OF CRIMES AND SPECIFIC PROCEDURES

Crimes under articles 25 *ter* and *25 sexies* of the Decree are examined below.

Particularly, the following information is provided for each type of crime:

- a description of the case at hand and the individuals who may have possibly committed a crime;
- possible areas at risk of a crime being committed;
- sensitive company processes;
- some examples of committed crimes;
- the procedures and controls required by the Company to prevent the crimes in the Decree from being committed.

Note that the sensitive activities listed in this Section are at risk of the tax crimes examined in Special Section A being committed. Individuals protected by corporate penal provisions and tax penalties are different. False financial reporting safeguards the authenticity of information intended for a wide range of individuals who are interested in the Entity's financial situation, while tax crimes safeguard the State's interest in tax collection. However, the falsifications, alterations and general inaccuracies of taxpayers are inevitably reflected in their tax returns, thus creating a financial situation that differs from the real one.

False corporate reports and false corporate reports to the detriment of shareholders and creditors (articles 2621, 2621 *bis* and 2622 of the civil code)

Description of the case in point:

There are two criminal cases (the first is a violation and the second a crime) where in both cases the typical conduct is almost completely the same, the difference being dependent on whether or not the Company's shareholders or creditors have suffered property damage.

These two criminal acts are carried out by entering in the annual reports, reports or other corporate documents required by law and intended for the shareholders or the public, significant material facts that

are untrue - even if they are under examination - and that could mislead others with regard to the income, assets and liabilities and financial situation of the company or the group to which it belongs, as required by law.

It should be noted that the conduct must be oriented towards obtaining undue profit, not only for the Entity but also for oneself or for others.

Individuals who could commit this crime are Directors, General Managers and Statutory Auditors.

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

- Management of General Accounting:
  - when the book entries are recorded in general accounting;
  - when the accounting data entered into the system are checked.
- Preparing the annual reports or the statements of assets and liabilities for extraordinary operations (mergers, spin-offs, reduction in capital);
  - when the accounting data needed to prepare a draft of the document to submit to the Board of Directors for approval are collected, grouped together and evaluated;
  - when preparing the reports attached to the income statement and assets and liabilities statement (Directors' Report and Explanatory Note), to be submitted to the Board of Directors for approval.

Some examples of committed crimes

The Board of Directors is not aware of the recommendation by the Head of Administration to allocate funds to the reserve for doubtful debts due to a customer's crisis situation, and enters an amount of receivables that is higher than required; this in order to prevent showing a loss that would require taking measures involving share capital.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- The annual report and the directors' report are drawn up according to specific company procedures which:
  a) clearly state the data and news that each department must provide through its managers to prepare the required reports, the criteria to process the required data as well as the timetable for each department concerned to submit its data to the departments heads;
  b) require that data and information be sent to the requesting department through the computer system, in order to trace each step and identify the individuals who entered the data into the system.
- A draft of the annual report and the auditing company's report must promptly be made available to all the members of the Board of Directors, while providing suitable documentation proving that said documents were delivered.

- Signing by the top company executive of a letter of assurance or indemnity requested by the auditing company.
- Procedures regarding coordination meetings of the various monitoring bodies.
- Systematic reporting to the Supervisory Committee of any assignment or intended assignment to the auditing company or to companies associated with it, other than those regarding the certification of the annual report.
- Sending the Committee the assessments concerning the selection of the auditing company.

Together with the existing procedures, the following additional controls are implemented:

- Information and training programs to be planned for all the managers of the departments involved in drawing up the annual report and other company reports, concerning the basics of the annual report as well as its legal and accounting problems. Refresher courses on changes in their fields of expertise.
- A clear, timed procedure for the departments mentioned above to determine which data and news need to be passed on to the administration department.
- Expected periodical information flows among monitoring bodies (Board of Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing Director, Chief Executive Officer) of the Company (meetings), also to verify that the corporate and *corporate governance* rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.1 False prospectuses (Art. 173 *bis* of the Consolidated Law on Finance)

Description of the case in point

This type of conduct consists in entering false information or concealing data and news for the purpose of misleading the recipients of prospectuses to encourage an investment or to accept an offer on regulated markets, or during takeover bids or public offers for the exchange of shares.

This offence can be committed by the Directors.

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

Preparing the prospectuses with a view to carrying out the above-mentioned transactions:

- when collecting, grouping and evaluating the data concerning the income statement and the statement of assets and liabilities needed to prepare a draft of the document to submit to the Board of Directors for approval;
- when preparing the reports to be submitted to the Board of Directors for approval.

Some examples of committed crimes

Any act or omission by Directors who, through their direct collaborators, can provide false information and/or conceal data and news aimed at misleading the recipients of the information.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- To prevent crimes from being committed, the following internal rules/procedures have been established:
  a) checking that data and information from internal sources are correct, and naming the source of external data and information;
  b) selecting an officer in charge of drawing up each prospectus;
  c) divulging the Principles of Conduct on the subject as provided for in this Model (see Annex) (hereinafter "**Principles of Conduct**") throughout the entire corporate organization so that the Directors, management and all employees can fully and properly collaborate with the monitoring bodies;
  d) setting up internal sanctioning mechanisms for those individuals who do not comply with the above-mentioned rules;
  e) reporting to the Committee by the officer in charge of the transaction, for each initiative requiring the drawing up and publication of prospectuses.

Together with the existing procedures, the following additional controls are implemented:

- periodical information and training programs for all Directors, management and employees, concerning the rules of corporate governance and corporate crimes and administrative offences;
- checking that the current system of delegation of powers and power of attorney is consistent with *corporate governance*;
- periodical information flows among monitoring bodies (Board of Statutory Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing Director, Chief Executive Officer) of the Company (meetings), to verify that the corporate and *corporate governance* rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.2 False reports and notifications by statutory auditors (art. 27 of Leg. Decree 39/2010)

The crime consists in statutory auditors making false statements or concealing information regarding the company's profits and losses, assets and liabilities and financial situation for the purpose of obtaining undue profit for themselves or for others.

The sanction is more serious if the conduct has caused the recipients of the notifications to suffer property damage.

The case in point was introduced by Legislative Decree 39/2010, which at the same time repealed art. 2624 of the civil code, which, as explicitly mentioned in art. 25 *ter*, initially provided for the crime.

Repealing the civil code article without adding art.25 *ter* with reference to the new case set forth in art. 27 of Legislative Decree 39/2010 should result in the non-applicability of the administrative sanctions under the Decree to the new crime of false reports or notifications by statutory auditors. Nonetheless and for the sake of prudence, the lack of legal precedents on this matter leads us to also take this case into account.

The perpetrators are the managers of the Auditing Company (crime that can only be committed by certain people) but the members of FATA's management boards and employees can be complicit in the crime. It is in fact possible to surmise, according to art. 110 of the criminal code, the complicity of the directors or auditors or other individuals of the audited company, who determined or instigated the illegal conduct of the auditing company manager.

Description of the case in point

The crime consists in auditors making false statements or concealing information regarding the company's profits and losses, assets and liabilities and financial situation.

This offence can be committed by the managers of the Auditing Company but FATA's management boards and employees can be complicit in the crime.

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

- Management of general accounting;
- Managing relations with shareholders, the Board of Statutory Auditors and the Auditing Company concerning the monitoring of administration and accounting as well as the annual report.

Some examples of committed crimes

Directors, auditors or other individuals of the company are complicit if they determined or instigated the illegal conduct of the Auditing Company.

Procedures and Checks

Given the particular nature of the case in point, the possible checks are those provided to prevent the crime of false corporate reporting.

6.3 Obstruction of audit (Art. 2625 of the civil code)

Description of the case in point

This conduct consists in preventing or hindering by concealing documents or other similar means the auditing activity that is legally conferred on the shareholders or other company boards.

This offence can be committed by the Directors.

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

- Management of general accounting;
- Managing relations with shareholders, the Board of Statutory Auditors and the Auditing Company concerning the monitoring of administration and accounting as well as the annual report.

Some examples of committed crimes

The conduct of the Directors, who can use their own direct collaborators, can translate into a failure to provide a member of the Board of Statutory Auditors with the documents he or she requests in the performance of his or her auditing activities, such as for example the documents concerning the legal actions brought by the company to recover receivables.

Procedures and Checks

Distribution of the Code of Ethics to the Company's top management figures and employees.

To prevent crimes from being committed, the following internal rules/procedures have been established:

- sending the Board of Statutory Auditors, sufficiently in advance, all the documents regarding the matters on the agenda of the meetings of the shareholders or Board of Directors, or on which the Board has to express an opinion according to the law;
- placing at the disposal of the monitoring bodies (Board of Statutory Auditors, Auditing Company, Supervisory Committee) all the documentation they require to perform their audits;
- divulging the Principles of Conduct throughout the entire corporate organization so that the Directors, management and all employees can fully and properly collaborate with the monitoring bodies;
- setting up internal sanctioning mechanisms for those individuals who do not comply with the above-mentioned rules.

Together with the existing procedures, the following additional controls are implemented:

- periodical information and training programs for all Directors, management and employees, concerning the rules of *corporate governance* and corporate crimes and administrative offences;
- checking that the current system of delegation of powers and power of attorney is consistent with *corporate governance*;
- periodical information flows among monitoring bodies (Board of Statutory Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing

Director, Chief Executive Officer) of the Company (meetings), to verify that the corporate and *corporate governance* rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.4 Unlawful transactions involving own shares or shareholdings or those belonging to the controlling company (art. 2628 of the civil code)

Description of the case in point

This crime consists in purchasing or subscribing shares or shareholdings of the controlling company that is damaging to the share capital and reserves that by law cannot be distributed.

Note that if the share capital or the reserves are re-established before the term for the approval of the annual report for the year in which the conduct occurred, the crime is null.

This offence can be committed by the Directors in connection with the shares.

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

Management of securities portfolio during ordinary purchase/sale of securities.

Some examples of committed crimes

The Board of Directors purchases or subscribes own shares without complying with the provisions in art. 2357 of the civil code, thus damaging the company's property.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- Formalization of procedures for the purchase of both own shares and shareholdings in controlling companies by group companies. Note that the purchase of said shareholdings must always take place within the limits set forth in the Civil Code and subject to authorization by the shareholders.
- Setting up internal sanctioning mechanisms for those individuals of the organization who do not comply with the above-mentioned rules.

Together with the existing procedures, the following additional controls are implemented:

- periodical information and training programs for all Directors, management and employees, concerning the rules of *corporate governance* and corporate law;
- checking that the current system of delegation of powers and power of attorney is consistent with *corporate governance*;
- expected periodical information flows among monitoring bodies (Board of Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Chief Executive Officer, Chairman) of the Company (meetings), to verify that the corporate and *corporate governance* rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.5 Transactions that are detrimental to creditors (Art. 2629 of the civil code)

Description of the case in point

This crime occurs when, in violation of the provisions of the law that protects creditors, reductions in share capital or mergers with other companies or spin-offs take place that cause harm to creditors.

Note that if the creditors receive compensation before going to court, the crime is null.

Individuals who could commit this crime are the Directors

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

Preparing statements of assets and liabilities for the purpose of carrying out extraordinary transactions (i.e. mergers, spin-offs).

Some examples of committed crimes

The Directors arrange an extraordinary merger with a company that is significantly indebted without complying with the procedure in art. 2503 of the civil code that protects creditors.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- Extraordinary transactions must always take place in accordance with the rules set forth in the Civil Code.
- Setting up internal sanctioning mechanisms for those individuals of the organization who do not comply with the above-mentioned rules.
- Together with the existing procedures, the following additional controls are implemented:
- periodical information and training programs for all Directors, management and employees, concerning the rules of *corporate governance* and corporate law;
- checking that the current system of delegation of powers and power of attorney is consistent with *corporate governance*;
- expected periodical information flows among monitoring bodies (Board of Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing Director, Chief Executive Officer) of the Company (meetings), to verify that the corporate and *corporate governance* rules are being complied with;
- regulating the procedure to be followed if any irregularities are found during the monitoring activities.

6.6 Failure to report conflicts of interest (Art. 2629 *bis* of the civil code

Description of the case in point

This occurs when a member of the Board of Directors or of the Management Board fails to comply with the obligation to report his/her interest in a given corporate transaction to the other members of the Board and to the Auditors, thereby damaging the company or a third party.

Individuals who could commit this crime are the Directors

At-risk areas

Directors of the board

Sensitive company processes

Resolutions of the Board of Directors

Some examples of committed crimes

A Director fails to make his/her interest in a given transaction known and does not abstain from voting on the resolution.

Procedures and Checks

Distribution of the Code of Ethics to top management figures and employees.

In addition to the existing procedures, periodical information and training programs are organized for all Directors, management and employees, concerning the rules of *corporate governance* and corporate law.

6.7 Undue return of capital contributions (art. 2626 of the civil code) and unlawful distribution of profits and reserves (art. 2627 of the civil code)

Description of the case in point

Undue return of capital contributions

Typical conduct consists in returning contributions to shareholders or releasing them from the obligation of making them, either openly or in a feigned manner, with the exception of cases of legitimate reduction of share capital.

Individuals who could commit this crime are the Directors (crime that can only be committed by certain people). However, according to the general rules in article 110 and subsequent articles of the criminal code, shareholders who instigate or assist the Directors could be guilty of complicity.

Unlawful distribution of profits and reserves

The criminal conduct of this crime, which is a technical offence, lies in the distribution of profits or advance payments on profits that have not actually materialized or that by law must be allocated to reserves, or in other words the distribution of reserves, even those that do not contain profits, which cannot be legally distributed.

Note that if the profits or the reserves are re-established before the term for the approval of the annual report, the crime is null.

Individuals who could commit this crime are the Directors (crime that can only be committed by certain people).

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

- Reduction in share capital;

- Distribution of profits or advance payments on profits;
- Distribution of reserves

Some examples of committed crimes

Undue return of capital contributions

The Company's shareholders, following a proposal by the Board of Directors, resolve to offset a debt that a shareholder owes the company with a contribution in capital owed to the company by the shareholder, essentially performing an undue return of a capital contribution.

Unlawful distribution of profits and reserves

The Company's shareholders, following a proposal by the Board of Directors, resolve to distribute dividends that do not represent the profit for the financial year but are funds that cannot be distributed because they are legally earmarked for legal reserves.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- The return of capital contributions and the distribution of profits or reserves must both take place in compliance with the law and the rules of procedure.
- If the above-mentioned transactions lead to reductions of share capital, they must be promptly reported to the creditors in order to obtain their authorization as provided for in the Civil Code.
- Setting up internal sanctioning mechanisms for those individuals of the organization who do not comply with the above-mentioned rules.
- Together with the existing procedures, the following additional controls are implemented:
- periodical information and training programs for all Directors, management and employees, concerning the rules of *corporate governance* and corporate law;
- checking that the current system of delegation of powers and power of attorney is consistent with *corporate governance*;
- periodical information flows among monitoring bodies (Board of Statutory Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing Director, Chief Executive Officer) of the Company (meetings), to verify that the corporate and *corporate governance* rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.8 Fictitious capital (Art. 2632 of the civil code)

Description of the case in point

This crime occurs when:

- the share capital is fictitiously created or increased by conferment of shares or shareholdings in an amount that is less than their face value;
- shares or shareholdings are reciprocally subscribed;
- contributions in kind, receivables or property of the company are significantly overvalued in the case of transformation.

Note that failure by the Directors and Auditors to check and possibly review the contributions in kind contained in the estimate report drawn up by the court-appointed expert is not an offence.

Individuals who could commit this crime are:

Directors or Contributing Shareholders (crime that can only be committed by certain people).

At-risk areas

- Administration, planning and control
- Financial Management;
- Top Management.

Sensitive company processes

- Preparing the annual reports, or the statements of assets and liabilities for extraordinary operations (mergers, spin-offs, increases in capital) when the accounting data needed to prepare a draft of the document to submit to the Board of Directors for approval are collected, grouped together and evaluated;
- Increases in capital.

Some examples of committed crimes

The Directors arrange for an increase in share capital by offering shares whose value is less than the declared one.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- Transactions involving the creation and increase of share capital must always take place in compliance with the law and the rules of procedure.
- Setting up internal sanctioning mechanisms for those individuals of the organization who do not comply with the above-mentioned rules.

Together with the existing procedures, the following additional controls are implemented:

- periodical information and training programs for all Directors, management and employees, concerning the rules of corporate governance and corporate law;
- checking that the current system of delegation of powers and power of attorney is consistent with corporate governance;
- periodical information flows among monitoring bodies (Board of Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing Director, Chief Executive Officer) of the Company (meetings), to verify that the corporate and corporate governance rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.9 Bribery among private individuals (Art. 2635 of the civil code)

For this type of crime, please refer to Special Section A.

6.10 Undue influence in general shareholders' meetings (Art. 2636 of the civil code)

Description of the case in point

Typical conduct consists in using sham transactions or fraud to create a shareholder majority for the purpose of wrongful gain for oneself or for others.

This is considered to be a "common offence", and therefore can be committed by anyone, including by individuals outside the Company.

At-risk areas

Top Management

Sensitive company processes

Preparing the annual report and the statements of assets and liabilities:

- in the case of extraordinary transactions (mergers, spin-offs, reductions in capital);
- in the case of projects, schedules and documentation to be submitted to the shareholders for approval.

Some examples of committed crimes

The Company's Board of Directors, for the purpose of obtaining a favorable decision from the shareholders and the decisive vote of the majority shareholder, prepares and presents altered documents during the shareholders' meeting to make the economic and financial situation of a company that the Board intends to acquire look better than it actually is, in order to indirectly profit from this.

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- Rules of procedure that regulate the participation and running of the meetings and the majority required to adopt resolutions.

Together with the existing procedures, the following additional controls are implemented:

- periodical information and training programs for all Directors, management and employees, concerning the rules of corporate governance and corporate law;
- periodical information flows among monitoring bodies (Board of Auditors, Auditing Company, Supervisory Committee) and management bodies (Board of Directors, Managing Director, Chief Executive Officer) of the Company (meetings), to verify that the corporate and corporate governance rules are being complied with. Regulation of the procedure to be followed if any irregularities are found during the monitoring activities.

6.11 Insider trading (art. 184 of the Consolidated Law on Finance)

Description of the case in point

Typical conduct consists in divulging and/or using - either directly or indirectly - insider information that an individual has come across during his/her professional activity for the purpose of performing transactions on the financial instruments to which the information refers.

At-risk areas

- Top management
- Management boards;
- Management and employees operating in at-risk areas.

Sensitive company processes

- Preparing the annual reports, statements of assets and liabilities and prospectuses for extraordinary transactions (mergers, spin-offs, capital transactions, acquisitions);
- Preparing multiyear programs, annual budgets and project budgets, schedules and associated documentation.

Some examples of committed crimes

Information acquired through one's job is used for direct or indirect trading - either for oneself or for others - on financial instruments (purchase, sale, repurchase, swap, etc.), or this information is divulged to others with no relation to the job, position or office (sharing of data needed to prepare the consolidated annual report among company groups is therefore not included).

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- Prohibiting personal transactions for oneself or for others using insider information acquired in relation to one's professional duties.
- To prevent crimes from being committed, the following internal rules/procedures have been established:
  - managing, sharing, processing and protecting insider information, including by means of access tracing mechanisms;
  - establishing the criteria to identify insider information;
  - identifying the relevant persons and setting up a register of relevant persons together with someone to manage it;
  - informing relevant persons concerning the legal and regulatory obligations deriving from having access to insider information;
  - setting up a committee to verify and monitor how insider information is divulged;
  - procedures to create and divulge news concerning the company, and identifying the individuals responsible for verifying that the information is correct and can be made known.

In addition to the existing procedures, periodical information and training programs are organized for all Directors, *management* and employees, concerning the rules of *corporate governance* and corporate law.

6.12 Market manipulation (art. 185 of the Consolidated Law on Finance)

Description of the case in point

Typical conduct involves divulging - by any means (including Internet) - misleading or false information, items or news that could be potentially deceptive in regard to financial instruments; this crime can also be committed in the case of transactions (trade orders) that provide or could provide information that is equally deceptive or that leads to irregular market prices being set.

At-risk areas

- Top Management
- Management boards
- Management and employees operating in at-risk areas

Sensitive company processes

- Preparing the annual reports, statements of assets and liabilities and prospectuses for extraordinary transactions (mergers, spin-offs, capital transactions, acquisitions) and other corporate reports;

- Preparing multiyear programs, annual budgets and project budgets, schedules and associated documentation;
- Periodical reporting to financial markets;
- Programs for the purchase of own shares and transactions on own financial instruments.

Some examples of committed crimes

Misleading information is disseminated (via market reports, board resolutions, annual report and periodical statements) that conceals the company's real situation (i.e. financial instability) (*information-based manipulation*); actions are taken by one or more people for the purpose of directly or indirectly setting unfair purchase and sale prices (*market-based manipulation*).

Procedures and Checks

- Distribution of the Code of Ethics to the Company's top management figures and employees.
- Prohibiting personal transactions for oneself or for others using insider information acquired in relation to one's professional duties.
- Prohibiting the dissemination of misleading information regarding financial instruments or other circumstances that could even potentially influence the price of the financial instruments.
- To prevent crimes from being committed, the following internal rules/procedures have been established:
  - conduct of corporate representatives with access to insider information, with particular reference to the obligations of reporting and conduct concerning transactions involving financial instruments;
  - procedures to create and divulge news concerning the company, and identifying the individuals responsible for verifying that the information is correct and can be made known;
  - transactions involving company securities, explicitly prohibiting anyone from operating outside of the authorized programs;
  - specific contractual precautions aimed at regulating the processing of and access to insider information by consultants/*partners* (confidentiality clause).

In addition to the existing procedures, periodical information and training programs are organized for all Directors, *management* and employees, concerning the rules of *corporate governance* and corporate law.

SPECIAL SECTION "C"

Areas where the crimes of manslaughter and unintentional serious or very serious injury can be committed in violation of the obligations to safeguard health and safety in the workplace as per art. 25 *septies* of Legislative Decree 231/2001

1. PURPOSE

Special Section C aims to regulate conduct to prevent the crimes in art. 25 *septies* of the Decree from being committed, by implementing a "*corporate system*" in accordance with the obligations in art. 30 of the Consolidated Law on Safety (T.U.S.: Decree Law 81/2008) based on:

- a company safety policy;
- risk analysis;
- procedures and instructions of conduct;
- personnel training and education;
- self-monitoring (internal inspections);
- formal recording of activities performed;
- periodical review of improvement goals by top management.

FATA has developed and implemented its own corporate system that is consistent with the above-mentioned requirements, obtaining ISO 45001:2018 certification in October 2020, published in the International Organization for Standardization of Geneva in 2018. The rules of conduct and the monitoring protocols described in this Special Section contain what is described in more detail in the "*Integrated management system for health, safety and the environment*" drawn up by FATA.

2. TYPES OF CRIMES

Art. 300 of Legislative Decree 81/2008 "*Implementation of article 1 of Law 123 of August 3, 2007, concerning the safeguarding of health and safety in the workplace*" and subsequent modifications, has added art. 25 *septies* to the Decree, which extends the administrative liability of legal entities to include the following crimes:

- Manslaughter (art. 589 of the penal code)
- Unintentional personal injury (art. 590 of the penal code)

committed in violation of the regulations governing accident prevention and the safeguarding of health and safety in the workplace.

In addition to the violation of regulations governing the safeguarding of health and safety in the workplace, which is dealt with in this Special Section, this can also include organized criminal activity. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

3. SENSITIVE PROCESSES

The activities that are at risk of the above-mentioned crimes being committed are potentially all those that take place in the Company's workplaces (HQ, plants, jobsites, etc.) and which require the presence of workers, and whose identification and analysis match the assessment of work-related risks carried out by FATA in compliance with the obligations set forth in Legislative Decree 81/2008.

4. RECIPIENTS

This section of the Model is intended for company individuals (the "**Recipients**") who are required to apply and/or comply with it when performing At-risk Activities in order to prevent conduct that is conducive to the perpetration of the crimes in art. 25 *septies* of the Decree.

The Recipients, who have different obligations depending on their role and responsibilities within the company, are listed below:

- Employer;
- Executives;
- Contractors;
- Supervisors;
- Company doctor;
- Employees;
- Supervisory Committee

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

5. GENERAL RULES OF CONDUCT

The system in general

This section sets out the general principles to prevent the mentioned crimes and conduct, thus protecting the health and safety of workers.

To this end, the Company has to set up an internal control system and issue internal procedures and provisions to regulate the above-mentioned subject matter (provisions that encourage the people in charge to take action, that govern preventive, periodical medical examinations and manage results; provisions to deal with first aid, emergencies, evacuation and fire prevention, and administrative management of accident and occupational disease records):

Requirements and skills

- Formal appointment of the Head of the Prevention and Protection Department (RSPP), company doctor, first aiders, fire prevention operators and emergency responders.
- Identification of individuals to ensure that maintenance-improvement measures are being implemented.
- The RSPP and the company doctor must possess the professional skills and requirements in terms of Prevention and Protection.
- The company doctor must take part in organizing environmental monitoring and receive a copy of the results.

Information

- Informing employees and new hires as to specific company risks.
- Proof that safety information has been provided and drawing up minutes of meetings.
- Formal documentation containing information and instructions for the use of work equipment.
- Planning of periodical meetings among workplace safety departments.
- Information on the appointment of the RSPP, company doctor and people in charge of specific tasks.
- Involving the RSPP and/or company doctor in preparing the information;
- Involving the Worker Safety Representative in organizing risk detection and assessment and appointing the operators.

Training

- Training of all Employees in workplace safety.

- Distributing assessment questionnaires.
- Ensuring that risk training is suited to the work that is actually assigned to the worker.
- Preparing a specific training plan for workers exposed to serious, immediate risks.
- Preventive, additional and specific training for workers who change jobs and are transferred.
- Participation of the RSPP and/or company doctor in drawing up the training plan.
- Specific training for operators in specific prevention and protection duties.
- Periodical evacuation drills with associated reports.

Registers and other documents

- Updating the accident register and the occupational disease register.
- Preparing a register of those exposed to carcinogens and mutagens.
- Documentary evidence of joint visits to workplaces by the RRSP and the company doctor.
- Keeping a log of workplace safety and hygiene obligations.
- The risk assessment document must indicate the instruments and methods used to make the assessment and must contain the schedule of measures to maintain and improve them.

Meetings

Periodical, formally convened meetings among the departments involved, which the Supervisory Committee may attend, with the associated report.

General Rules of Conduct

Anyone who, because of their business or job, is in a condition to apply and comply with all aspects of the safety regulations, is expressly prohibited from implementing or giving rise to conduct that could directly or indirectly lead to crimes of manslaughter and unintentional serious or very serious injury committed in violation of accident prevention regulations concerning the protection of workplace health and safety.

In regard to all of the above and considering their specific position within the company (role and responsibility) the above-mentioned subjects are required to fulfill the following obligations:

Employers shall:

Appointment of managers:

- appoint the head and operators of the Prevention and Protection Department (RRSP and ASPP), which can be either internal or external to the company;

Risk Assessment:

- assess the risks to the safety and health of workers, including groups of workers exposed to particular risks, risks linked to the use of equipment and work materials, and those related to the workplace;
- at the end of the assessment, prepare a document (to be kept at the company or production facility) containing:
    - a risk assessment report for workplace health and safety, specifying the criteria used for the assessment;
    - identify the prevention and protection measures and personal protection devices resulting from the risk assessment for worker health and safety;

- a program of measures that are considered appropriate to ensure that safety levels improve over time;

In situations of mandatory health surveillance, the assessment and preparation of the document must be carried out in collaboration with the RSPP and the company doctor after consulting the Worker Safety Representative (RLS), and need to be repeated if significant changes in terms of worker safety and health are made to the production process.

Employers and Executives shall:

Appointment of managers:

- appoint the head and operators of the Prevention and Protection Department (RRSP and ASPP), which can be either internal or external to the company;
- appoint the company doctor;
- select the workers to implement measures for fire prevention and firefighting, worker evacuation in case of serious immediate danger, rescue, first aid and dealing with emergencies in general;
- assign workers duties that are in keeping with their skills and health condition.

Risk Assessment:

- assess the risks to the safety and health of workers, including groups of workers exposed to particular risks, risks linked to the use of equipment and work materials, and those related to the workplace;
- at the end of the assessment, prepare a document (to be kept at the company or production facility) containing:
  - a risk assessment report for workplace health and safety, specifying the criteria used for the assessment;
  - identify the prevention and protection measures and personal protection devices resulting from the risk assessment for worker health and safety;
  - a program of measures that are considered appropriate to ensure that safety levels improve over time.

  In situations of mandatory health surveillance, the assessment and preparation of the document must be carried out in collaboration with the RSPP and the company doctor after consulting the RLS, and need to be repeated if significant changes in terms of worker safety and health are made to the production process;

- organize periodical meetings among workplace safety departments;
- consult the RLS on: risk assessment, identifying, programming, implementing and checking prevention within the Company, appointing operators for accident prevention, fire prevention, first aid, worker evacuation; and on planning the training of workers in charge of handling emergencies.

Prevention measures

- adopt the measures required for worker safety and health, particularly:
  - select the workers to implement measures for fire prevention and firefighting, worker evacuation in case of serious immediate danger, rescue, first aid and dealing with emergencies in general;
  - update prevention measures according to organizational and production changes affecting workplace health and safety, or depending on the degree of evolution of prevention and protection techniques;

- provide the workers with the required personal protection equipment in agreement with the RSPP;
- take appropriate steps to prevent the technical measures adopted from causing risks to the health of the population or degrading the external environment;
- apply all the measures required to prevent fires and evacuate workers, as well as in the case of serious, immediate danger; these measures must be suited to the type of work, the size of the company or production unit and the number of people on the site.

Information

- allow workers to check, through the RLS, that the measures to protect safety and health have been applied, and allow the RLS to access the information and company documentation related to risk assessment, the associated prevention measures, and those regarding hazardous substances and preparations, machines, plants, organization and work environment, accidents and occupational diseases;
- inform employees and new hires (including temporary workers, trainees and those under project-based contracts) regarding specific company risks, their consequences and the prevention and protection measures that were adopted;
- provide proof that information was provided for first aid, emergencies, evacuation and fire prevention; draw up reports of any meetings;
- provide information on the appointment of the RSPP, company doctor and people in charge of specific tasks for first aid, rescue, evacuation and fire prevention to employees and new hires (including temporary workers, trainees and those under project-based contracts);
- produce formal documentation containing information and instructions for the use of work equipment provided for employees;
- involve the RSPP and/or company doctor in preparing the information;

Training

- provide workplace safety training for all Employees;
- have the RSPP and/or company doctor take part in drawing up the training plan;
- distribute assessment questionnaires;
- ensure that risk training is suited to the work that is actually assigned to the worker;
- prepare a specific training plan for workers exposed to serious, immediate risks;
- provide preventive, additional and specific training for workers who change jobs and are transferred;
- provide specific training for operators with specific prevention and protection duties (fire prevention, evacuation, first aid);
- schedule periodical evacuation drills with proof that they have been carried out (recording the completed drill and indicating the participants, how it was done and the results);
- provide specific training for the RLS.

Registers and other documents

- keep a register listing in chronological order the workplace accidents that entail at least one day of absence from work;
- prepare and keep a register of workers exposed to carcinogens or mutagens.

Meetings

- plan periodical meetings among the departments involved, which the Supervisory Committee may attend, by formal convocation and with the associated report signed by the participants;

Contracts

- **the employer commissioning the work and the contractor** shall prepare a unified document assessing the interference risks (DUVRI), indicating the measures that were adopted to eliminate the interferences. This document must be attached to the major or minor contract for services or work;
- **as employer, the Company** shall**:**
  - in the presence of subcontractors, set out the procedures to manage and coordinate the subcontracted work;
  - by registering with the chamber of commerce, industry and crafts, check that the contracting companies or self-employed workers are technically and professionally capable of performing the major or minor commissioned work;
  - in supply and service contracts and subcontracts, indicate the work safety costs and determine the management of workplace safety-related obligations for subcontracts. On request, the RLS and the trade unions can have access to these data;
  - provide contractors with detailed information concerning the specific risks of the environment in which they will be working, and regarding the prevention and emergency measures adopted for their activity;
  - prepare and update the list of companies contracted to operate on its sites;
  - formalize the procedures to manage and coordinate work under written contracts containing references to the obligations in art. 26 of Legislative Decree 81/08, such as checking by the employer that the contracted companies are technically and professionally suited to perform the work that is awarded to them under contract;
  - cooperate in implementing measures to prevent and protect against workplace risks that impact the contracted work;

- **as contractor, the Company shall:**
  - ask the companies for which it works as a contractor for information on specific risks and the preventive measures these companies have adopted;
  - prepare and update the list of companies for which it operates as a contractor;

1. **the Supervisors** shall:

- make sure that only the workers who have received adequate instructions can enter the areas where they are exposed to serious, specific risks;
- require that each worker comply with current regulations and company rules in terms of safety and hygiene in the workplace, as well as using the collective and individual protection devices;
- require that the company doctor comply with the obligations specified in workplace safety regulations, informing him/her of the processes and risks connected with production;
- adopt measures to control risky situations during emergencies, instructing workers to leave their work station or hazardous area in case of serious, immediate and inevitable danger;
- inform workers exposed to serious and immediate risks as to the actual risks and the safety specifications that have been adopted;
- refrain from asking workers to resume their work in a situation of serious and immediate danger, except in duly justified cases;
- promptly report to the employer or executive any shortage of work means and equipment and personal protection devices, as well as any other hazardous conditions that arise while working.

2. **the company Doctor** shall:

- at the company or production facility, keep the medical and risk files of workers subject to health surveillance while safeguarding professional secrecy; a copy shall be given to the worker upon termination of employment, or if the worker requests a copy;
- work with the employer and with the department of prevention and protection on risk assessment, on implementing the measures to safeguard the health and physical and mental fitness of the workers, on training and informing the workers and organizing the first aid service;
- plan and carry out health surveillance;
- provide workers, and on request, the workers' safety representatives, with information on health surveillance;
- prepare written reports containing the anonymous, collective results of the health surveillance that was carried out;
- visit the work environments at least once a year or as required according to the risk assessment;

3. **the Workers** shall:

- comply with the provisions and instructions given by the employer, by the executives and by the supervisors to ensure collective and individual protection;
- immediately report to the employer, executive or supervisor, any shortages of the means and devices indicated in the previous items, as well as any other hazardous conditions of which workers may become aware, making a direct effort, within the scope of their abilities and possibilities, to eliminate or reduce said shortages or hazards in emergency situations while informing the RLS;
- not remove or modify the safety, warning or control devices without authorization;
- not carry out operations or maneuvers on their own initiative that are not part of their job description or that could jeopardize their own safety or that of other workers;
- correctly use the machinery, equipment, tools, hazardous substances and preparations, means of transportation and other work equipment, as well as the safety devices;
- appropriately use the protection devices provided;
- undergo the required medical examinations;
- contribute, together with the employer, the Executives and the supervisors, to fulfilling all the obligations required by the competent authority or that are necessary to safeguard the safety and health of workers while they are working.

6. ACTIVITIES OF THE SUPERVISORY COMMITTEE

In performing its activities, the Committee shall refer to the specific history of the Entity and its unique characteristics (previous violations, criminal proceedings, number of accidents and their seriousness, accident log, etc.).

The Committee shall verify the existence, the actual compliance with the real situation and the precise application of the items given below as examples:

Risk Assessment

- Workplace risk assessment document and associated updates;
- Asbestos risk assessment document;
- Fire risk assessment document;
- Chemical risk assessment document;
- Noise exposure assessment document;
- Document to assess manual load handling;
- Document to assess the risk of video terminals.

Formal requirements

- Board of directors' report with the name of the employer;
- Appointment of RSPP;
- Delegation and appointment of people to implement safety activities;
- Selection of RLS;
- Appointment of firefighting operators as first aiders and emergency responders;
- Minutes of periodical yearly prevention meetings and RLS consulting;
- Documentation confirming distribution of personal protection equipment

Fire prevention and emergency management

- Fire prevention certificate;
- Emergency and evacuation plan;
- Training certificates for firefighting, first aid and emergency management team;
- Test reports and emergency management;
- Register of checks and maintenance work performed on firefighting equipment (pursuant to Presidential Decree n. 37/98).

Training

- Training certificates and reports for supervisory personnel;
- Worker information and education reports;
- Training documentation for RLS and RSPP.

Procedural Documentation

- Management of major and minor contracts

Health surveillance

- Appointment of the company doctor;
- Health protocol - ascertaining worker fitness for the job;
- Report on the Doctor's site inspection

Technical documentation

- Planimetry and updated layout;
- Usability certificate of the premises;
- Declaration of Conformity of electrical system;
- Reporting and checking of the grounding system;
- Heat generator documentation and maintenance logbook;
- Operating and maintenance booklets for machines/equipment;
- Safety sheets of the chemical products that are used.

7. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The following information must reach the Committee:

Reports, repetitions and updates:

- risk assessment documents;

- documentation on the formal requirements to appoint the various managers (RSPP, MC) and those assigned special tasks (AI, PS, GE);
- fire prevention certificate and fire prevention register with the various updates;
- technical procedural documentation.

Event notification:

- all cases of workplace accidents (including minor ones);
- the results of safety checks of workplaces and equipment carried out by any external body;
- the results of safety checks of workplaces carried out by internal bodies.

SPECIAL SECTION "D"

Areas of business in which computer crimes could be committed, pursuant to article 24 *bis* of Legislative Decree 231/2001

1. PURPOSE

Special Section D refers to cases of computer crime as detailed below, which are included in the predicate offences of art. 24 *bis* of the Decree.

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

2. TYPES OF CRIMES

Law 48/2008 "*Ratification and implementation of the Cybercrime Convention of the Council of Europe, signed in Budapest on 23rd November 2001, and regulations to make the necessary changes to the national legal system",* extended the types of crimes that can create liability for the company to include the following:

- Forgery of electronic documents (Art. 491 *bis* of the penal code);
- Illegal access to IT or telematic systems (art. 615 *ter* of the penal code);
- Illegal possession, distribution and installation of equipment, codes and other means to access IT or telematic systems (Art. 615 *quater* of the penal code);
- Possession, distribution and installation of computer equipment, devices or programs aimed at damaging or interrupting an IT or telematic system (Art. 615 *quinquies* of the penal code);
- Illegal wiretapping, hindering or interruption of IT or telematic communication (Art. 617 *quater* of the penal code);
- Illegal possession, distribution and installation of equipment to wiretap, hinder or interrupt IT or telematic communication (art. 617 *quinquies* of the penal code);
- Damage to information, data or computer programs (art. 635 *bis* of the penal code);
- Damage to information, data or computer programs used by the State or other Public Entity, or that in any event are of service to the public (art. 635 *ter* of the penal code);
- Damage to IT or telematic systems (art. 635 *quater* of the penal code);
- Damage to public service IT or telematic systems (art. 635 *quinquies* of the penal code);
- Computer fraud of the entity that provides a certified e-mail service (art. 640 *quinquies* of the penal code);

The at-risk business areas in which the above-mentioned crimes could be committed are those related to the process of development, management and maintenance of the company's IT system and of the automated company procedures to manage data and information used in administration and production (example: general accounting, payroll and salaries, *Materials Requirements Planning*) and for the purpose of management control and strategic support.

3. SENSITIVE PROCESSES

The areas of the company in which there could be a risk of the above-mentioned computer-related crimes being committed, as per article 24 *bis* of the Decree are, theoretically, all those in which the activities are backed by IT and/or telematic systems for data processing and transmission (management, accounting, fiscal, etc.). The prevention of computer-related crimes must take place through suitable **organizational, technological and regulatory measures.**

As regards **sensitive activities**, with reference to the computer-related crimes stated in art. 24 *bis* of the Decree, any company activity that entails the management, maintenance and use of IT systems, databases and ICT platforms and structures in general can be theoretically considered at risk.

The macro business areas that are at risk are the following:

- company management IT systems;
- financial/management application service provider;
- processing of financial/management information;
- management and/or administration and/or maintenance of IT systems and IT systems for production;

The macro areas described above, which are exposed to a risk of computer crimes being committed as described in this Special Section, may also give rise to the same types of crimes being committed by criminal organizations. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

4. RECIPIENTS

This Special Section is intended for company individuals (**Recipients**) who work or could work in at-risk processes.

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

5. GENERAL RULES OF CONDUCT

According to the above-mentioned approaches, at-risk activities must be performed in compliance with the Code of Ethics, the rules of conduct and the fundamental goals of cyber safety indicated below, which FATA has set out:

- **Confidentiality**: guarantee that a given datum is protected against improper access and used exclusively by authorized individuals. Both the sending and memorization/storage of confidential information must be protected so that the information is accessible only to those who are authorized to know it;
- Wholeness: guarantee that each company datum is really the one that was originally entered into the **IT system** and that any change was legitimate. The information has to be guaranteed to be processed in such a way that it cannot be tampered with or modified by unauthorized individuals;
- **Availability**: guarantee of availability of company data depending on the requirements of process continuity and in compliance with the standards requiring that a history be kept.

In general, for activities that:

- involve the processing of data and information whose improper use can lead to fraud to the detriment of natural persons or corporate bodies (private organizations and, in particular, if the counterpart is employed with the Public Administration);
- require access to infrastructures, equipment or software which could lead to fraudulent conduct or actions;
- need to purchase or manage products and services connected with IT technologies;

it is necessary to:

- determine, approve, re-examine and check the application of internal procedures and operating instructions that set out the duties and job titles related to physical and logical safety;
- establish the levels of access and information that could be used or exchanged at the various functional levels;
- verify the use of the equipment and software infrastructure;

- keep logs of completed transactions.

To this end, the following procedures and monitoring and control elements shall be implemented to monitor the business activity:

- identifying the risks deriving from dealing with external parties (public organizations, customers, suppliers);
- establishing and divulging a suitable information safety policy through specific training and periodical review;
- establishing, applying, checking and periodically reviewing a suitable safety organization with:
  - specific assignment of responsibility for access authorization;
  - specific assignment of responsibilities for contracts with the authorities and specific interest groups;
- physical and logical access to ICT infrastructures limited only to people who are authorized under a contract;
- monitoring of ICT infrastructures (desktop and portable computers, networks, basic software), in terms of purchase and configuration change and management, checking their technical vulnerabilities, fixed supports (i.e. not computer terminal cases) and removable supports (i.e. back-up) to prevent their improper use by personnel or third parties, checking the dismantling, transfer of property or re-utilization of the equipment by company individuals or third parties;
- classification of information with the possibility of diversified access (registration of users, privilege management, *password* management), periodical update of profiles based on changes in job title and responsibilities, of personnel profiles and terms and conditions of use; checking that technological media are returned upon termination of a contract; checking access to user and system documentation, to program source codes and to development and test data;
- validation of input and output data by authorized individuals, and setting up a policy to encrypt data and manage encryption keys;
- monitoring and review of services provided by third parties and of changes to third-party services; for outsourcing services in particular, particular contractual clauses needed to be drawn up that obligate the supplier to conduct him/herself in accordance with the conduct required by the company. For example, if the *outsourcer* is required to manage the ICT infrastructure, checks need to be contractually provided for and accepted in order to verify:
  - infrastructure configuration management;
  - conduct and prevention actions implemented to reduce the risks of technical vulnerability, such as:
    - site allocation and layout;
    - physical safety measures;
    - access control;
    - protection against environmental factors;
    - management of *facilities*;
    - preparing work scheduling procedures;
    - infrastructure monitoring;
    - protection of sensitive documents;
    - *hardware* preventive maintenance;
- protection against malware that is able to commit fraudulent actions on proprietary ICT equipment.

6. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

In order for the Committee to perform its control and supervisory duties, the Company shall:

- systematically provide a list of instructions regarding security when using IT resources;

- report negative events regarding information security, indicating how the information is processed and providing an analysis of the causes and corrective actions undertaken to keep them from occurring again.

SPECIAL SECTION "E"

Section E.1 - Areas of business in which crimes could be committed in violation of the regulations to prevent the financial system from being used for money laundering, pursuant to article 25 *octies* of Legislative Decree 231/2001

Section E.2 - Areas of business in which crimes involving non-cash payment instruments could be committed, pursuant to article 25-*octies*. 1 of Legislative Decree 231/2001

SPECIAL SECTION E.1

Special Section E.1 refers to crimes committed in violation of the regulations to prevent the financial system from being used to launder money from criminal activities and to finance terrorism, referring to the cases of conduct stated in article 25 *octies* of the Decree.

The aim of this regulation is to ensure that all the people involved conduct themselves in a manner that complies with the Model in order to prevent the crimes specified by the legislature in the Third Anti-Money Laundering Directive (Leg. Decree 231/2007) from being committed.

Note that the tax crimes specified in Special Section A can be a sign of risk that the crimes stated in art.25 *octies* of the Decree could be committed.

1. SENSITIVE PROCESSES

Considering that FATA is not one of the entities listed in art. 11 and subsequent articles for whom the specific requirements set forth in Legislative Decree 231/2007 are intended, the corporate activities to be considered for the prevention of the predicate offences in question are those that concern relations with third parties and companies of the Danieli Group.

In this context, the main sensitive processes can be summarized as follows:

Relations with third parties

1. Purchase and/or sales contract with counterparts;
2. Financial transactions with counterparts;
3. Investments with counterparts;

Relations among Group companies

4. Purchase and/or sales contracts;
5. Management of financial flows;
6. Investments

The processes described above, which are exposed to the risk of the crimes of money laundering and possession of stolen goods being committed, as described in this Special Section, may also give rise to the same types of crimes committed by criminal organizations. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

2. RECIPIENTS

This section of the Model is intended for company individuals (the "**Recipients**") who, because of their position, role or corporate function, are required to apply or comply with it, in the performance of at-risk activities.

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

3. GENERAL RULES

The system in general

The aim of this Section is to ensure that anyone who is involved in activities where one of the specified crimes could be committed abide by the rules of conduct described herein for the purpose of preventing conduct that could directly or indirectly lead to the crimes of possession of stolen goods, money laundering and the use of illegal money, goods or benefits.

In particular, when performing these activities it is strictly prohibited to create, collaborate or give rise to types of conduct that taken individually or collectively, could directly or indirectly lead to crimes of possession of stolen goods, money laundering and the use of illegal money, goods or benefits.

Specific procedures and instructions

When performing operations that are pertinent to at-risk activities, in addition to the rules of the Model, the Recipients of this prevention system must comply with:

- applicable Italian and foreign legislation;
- Code of Ethics;
- internal control system (principles of *corporate governance*, company procedures and guidelines, documentation and provisions on organizational structure and management control system approved by the Board of Directors);
- regulations governing the administrative, accounting, financial and *reporting* systems of the Company;
- applicable laws, standards and regulations of market regulatory authorities (CONSOB and the Italian Stock Exchange in particular).

General Rules of Conduct

Anyone who, because of their business or job, is in a condition to apply and comply with legislation on money laundering, is expressly prohibited from implementing or giving rise to conduct that could directly or indirectly lead to crimes of possession of stolen goods, money laundering and the use of illegal money, goods or benefits, in violation of money laundering legislation.

The different positions and obligations of each individual are taken into consideration for sanctioning purposes.

Consequently, the above-mentioned individuals are explicitly obligated to:

- verify the commercial and professional reliability of suppliers and commercial/financial partners, based on certain significant indexes (i.e. damaging public data - protests, bankruptcy proceedings - or acquisition of commercial information on the company, shareholders and directors through specialized companies; extent of price disproportionateness compared to average market values, involvement of "*politically exposed people*"[13]);

[13] As set forth in art. 1 of the technical attachment of Legislative Decree 231/07 "Natural persons who hold or have held important public positions are: *a)* Heads of State, Heads of Government, Ministers and Deputy Ministers or Undersecretaries; *b)* Members of Parliament; *c)* Members of the Supreme Court, Constitutional Courts and other high-level judicial authorities whose decisions are not generally subject to further appeal except in exceptional circumstances; *d)* members of the courts of auditors and of the boards of directors of the central banks; *e)* ambassadors, chargés d'affaires and high-ranking officers of the armed forces; *f)* members of the boards of directors, management boards or supervisory committees of state-owned companies. None of the above-mentioned categories include medium and low-level government officials. The categories in letters *a)* to *e)* include European and international positions, where applicable. Direct family members means: *a)* spouses; *b)* children and their spouses; *c)* those who in the last five years have lived with the individuals indicated above; *d)* parents. Individuals with whom the people in article 1 are known to have a close relationship are: *a)* any natural person who is known to have joint beneficial ownership of legal entities or any other close business relationship with a person in art. 1; *b)* any natural person who is the sole beneficial owner of legal entities or legal persons known to have been created for the benefit of the person in art. 1".

- verify that payments are regular, and that the payment recipients/payers match the counterparts who are actually involved in the transactions;
- carry out formal, substantial checks of the company's financial flows, with reference to payments to third parties and payments/transactions among Group companies; these checks shall take into account the headquarters of the counterparty (i.e. tax havens, countries at risk of terrorism, etc.), of the credit institutions used (headquarters of the banks involved in the transactions and institutions without a permanent establishment in any country) and any corporate veils and trust companies used for extraordinary transactions or operations;
- check cash flow (to ensure it does not exceed the threshold for cash payments, possible use of a bearer or anonymous passbook to manage liquidity, etc.);
- establish the minimum requirements of bidders and set the criteria to evaluate the offers on *standard* contracts;
- select someone to draw up the technical specifications and evaluate the offers on *standard* contracts;
- select the body/unit in charge of performing the contract, indicating duties, roles and responsibilities;
- provide specific disciplinary rules regarding the prevention of money laundering;
- determine the criteria for the selection, stipulation and performance of agreements / *joint ventures* with other companies with a view to making investments. Transparency and traceability of agreements / *joint ventures* with other companies with a view to making investments;
- check the economic consistency of any investments made under a joint venture (in keeping with average market prices, use of trustworthy professionals for *due diligence* operations);
- check the degree of compliance of controlled companies with anti-money laundering measures and controls;
- apply specific preventive controls (protocols) which are also required for *market abuse* crimes;
- adopt suitable information programs for personnel considered to be exposed to the risk of money-laundering.

4. ACTIVITIES OF THE SUPERVISORY COMMITTEE

The Committee shall verify the existence, the actual compliance with the real situation and the precise application of the items given below as examples:

- commercial and professional reliability of suppliers and commercial/financial partners, based on certain significant indexes (i.e. price, product quality, conditions of the bidder, etc.);
- formal substantial checks of corporate financial flows;
- minimum requirements of bidders, setting the criteria to evaluate the offers on *standard* contracts;
- suitability of the person in charge of drawing up the technical specifications and evaluating the offers on *standard* contracts;
- suitability of the body/unit in charge of performing the contract, indicating duties, roles and responsibilities;
- suitability of the criteria for the selection, stipulation and performance of agreements / joint ventures with other companies with a view to making investments.

5. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The heads of the departments in question shall on a regular set basis inform the Committee of all abnormal situations and conduct that concern them, observed by anyone, and the transactions performed departing from the above-mentioned principles, with reference to the specific company processes that are at risk of a crime being committed, and together with the periodical flows indicated in Special Section A.

SPECIAL SECTION E.2

Special Section E2 deals with crimes involving non-cash payment instruments, and refers to the cases of conduct indicated in Art.25-*octies*. 1 of the Decree.

The aim of this regulation is to ensure that all the people involved conduct themselves in accordance with the Model in order to prevent the crimes involving non-cash payment instruments from being committed, as per Art.25 *octies*. 1 of the Decree.

1. SENSITIVE PROCESSES

The corporate activity to be considered for the purpose of preventing the predicate crimes in question is:

- Treasury Management

The processes described above, which are exposed to the risk of crimes involving non-cash payment instruments being committed as described in this Special Section, may also give rise to the same types of crimes being committed by criminal organizations. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

2. RECIPIENTS

This section of the Model is intended for company individuals (the "**Recipients**") who, because of their position, role or corporate function, are required to apply or comply with it, in the performance of at-risk activities.

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

3. GENERAL RULES

The system in general

The aim of this Section is to ensure that anyone who is involved in activities where one of the specified crimes could be committed abide by the rules of conduct described herein for the purpose of preventing conduct that could directly or indirectly lead to crimes involving non-cash payment instruments.

In particular, when performing these activities it is strictly prohibited to create, collaborate or give rise to types of conduct that taken individually or collectively, could directly or indirectly lead to the crimes of possession of stolen goods, money laundering and the use of illegal money, goods or benefits.

Specific procedures and instructions

When performing operations that are pertinent to at-risk activities, in addition to the rules of the Model, the Recipients of this prevention system must comply with:

- applicable Italian and foreign legislation;
- Code of Ethics;
- internal control system (principles of *corporate governance*, company procedures and guidelines, documentation and provisions on organizational structure and management control system approved by the Board of Directors);
- regulations governing the administrative, accounting, financial and *reporting* systems of the Company;

- applicable laws, standards and regulations of market regulatory authorities (CONSOB and the Italian Stock Exchange in particular).

General Rules of Conduct

Anyone involved in treasury management is strictly prohibited from implementing or giving rise to conduct that could directly or indirectly lead to crimes involving non-cash payment instruments.

The different positions and obligations of each individual are taken into consideration for sanctioning purposes.

Consequently, the above-mentioned individuals are explicitly obligated to:

- adopt any organizational and technical measure required to prevent any illicit use or forgery of non-cash payment instruments (tangible or intangible):
- use only payment channels and services that have been enabled according to the reference regulations;
- use only non-cash payment instruments of guaranteed legitimate origin and use;
- determine and register the payment instruments allowed by the Company, and for which it can guarantee ownership;
- periodically monitor non-cash payment instruments to ensure they are properly registered;
- identify and delegate authorized individuals to make payments using both cash and non-cash payment instruments (tangible or intangible) on behalf of the company.

It is also prohibited to:

- unduly use credit or debit cards that do not belong to you or any other similar document to withdraw cash or purchase goods or services, or any other non-cash payment instrument
- use computer equipment, devices or programs as non-cash payment instruments that are counterfeit or forged
- alter, forge or tamper with credit and debit cards or other non-cash payment instruments
- in any way alter the operation of an IT or telematic system, or in any way make changes without being entitled to do so, to data, information or programs if this produces a transfer of money, monetary value or virtual currency.

4. ACTIVITIES OF THE SUPERVISORY COMMITTEE

The Committee shall verify the existence, the actual compliance with the real situation and the precise application of the items given below as examples:

- use of non-cash payment instruments for which it is not possible to guarantee a legitimate origin and utilization

5. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The heads of the departments in question shall on a regular set basis inform the Committee of all abnormal situations and conduct that concern them, observed by anyone, and the transactions performed

departing from the above-mentioned principles, with reference to the specific company processes that are at risk of a crime being committed, and together with the periodical flows indicated in Special Section A.

SPECIAL SECTION "F"

Crimes by criminal organizations as per art. 24 *ter* of Legislative Decree 231/2001 (introduced by Law 94/2009), art.2, paragraph 29) and transnational crimes (pursuant to art. 10 of Law 146/2006)

1. PURPOSE

This Special Section refers to conduct by the Recipients of the Model, as better defined in the General Section, who are involved in activities where a crime could be committed by a criminal organization, either nationally and/or transnationally, that is among the predicate offences set forth in art. 24 *ter* of the Decree (introduced by art.2, paragraph 29 of Law 94/2009) and as required in art. 10 of Law 146/2006.

This Special Section aims to ensure that the above individuals conduct themselves in compliance with the principles stated herein, for the purpose of preventing said crimes from being committed.

2. TYPES OF CRIMES

Art. 2, par. 29 of Law 94/2009 added to art. 24 *ter* of the Decree, the administrative liability of entities in relation to crimes by criminal organizations (so-called "criminal association"):

- criminal conspiracy (art. 416, par. 1-6 of the penal code);
- Mafia-type conspiracy (art. 416 *bis* of the penal code);
- kidnapping for extortion purposes (art. 630 of the penal code);
- conspiracy to illegally traffic in narcotics or psychotropic drugs (art. 74 of Presidential Decree 309/1990);
- illegal manufacture, import, sale, transfer, possession and bearing of military or military-like weapons or parts thereof, explosives, illegal weapons and several common firing weapons, in places that are public or open to the public.

Art. 10 of Law 146/2006 previously specified the administrative liability of entities for crimes committed transnationally:

- criminal conspiracy (art. 416 of the penal code);
- Mafia-type conspiracy (art. 416 *bis* of the penal code);
- conspiracy to illegally traffic in narcotics or psychotropic drugs (art. 74 of Presidential Decree 309/1990);
- conspiracy to smuggle foreign processed tobacco (art. 291 *quater* of Presidential Decree 43/1973);
- migrant smuggling, for the crimes in art. 12, par. 3, 3 *bis*, 3 *ter* and 5 of the Consolidated Act as per Legislative Decree 286/1998.

For more details on the above crimes, please refer to Attachment 2 "Description of Predicate Crimes - Description of the case in point".

3. SENSITIVE PROCESSES

For crimes committed by criminal organizations, the company processes where a potential exposure to risk was determined are:

- Administration, planning and control
- Sales;
- Purchase of goods and services;
- Selection and management of personnel;
- Operative finance and cash management;
- Authorizations, concessions and relations with control bodies;
- Health and safety in the workplace;
- Environmental management;

- Management of information system;
- Professional consulting and services;
- Gifts, entertainment expenses and hospitality;
- Sponsorships, advertising initiatives and contributions.

Particular attention is to be paid to strategic, commercial and financial *partnerships*.

4. RECIPIENTS

This section of the Model is intended for company individuals (the "**Recipients**") who, because of their position, role or corporate function, are required to apply or comply with it, in the performance of at-risk activities.

The aim of this Section is to ensure that anyone who is involved in activities where one of the crimes specified herein could be committed, abide by the rules of conduct described herein for the purpose of preventing conduct that could directly or indirectly lead to organized crimes, both nationally and transnationally.

5. GENERAL RULES OF CONDUCT

This Special Section states that the Recipients are specifically prohibited from, as better described in the General Section, creating, working towards or giving rise to conduct, either nationally or transnationally:

- which - taken individually or collectively - could directly or indirectly integrate the crimes such as those mentioned in this Special Section (art. 24 *ter* of the Decree and art. 10 of Law 146/2006);
- which, although it does not actually constitute one of the crimes considered, could potentially become one;
- which is not in compliance with company procedures or not in line with the requirements set forth in this Model and the principles of the Code of Ethics.

All those who work on behalf of the Company shall act in compliance with the principles of integrity, prudence, fairness, transparency and honesty, fulfilling the following requirements:

- anyone, acting on behalf of FATA, coming into contact with third parties with which FATA intends to initiate commercial relations or with whom he/she is obligated to have institutional, social and political relations, or any other type of relations, has the obligation to:
  - inform said individuals of the commitments and obligations of the Code of Ethics;
  - adopt the necessary internal initiatives should the third parties refuse to conform to the Code of Ethics and observe the provisions contained therein;

- all relations with agents, intermediaries and commercial partners shall be based on principles of transparency and integrity, and require that the services and fees are in line with market practices, ascertaining that there are no aspects that could encourage crimes to be committed in Italy and abroad by third parties;
- constant, continuous verification of the fairness, effectiveness, consistency and compliance with the company's interests of the requested services rendered by or for third parties, in order to guarantee that only fair commercial, financial and consulting relations are set up and maintained that truly fulfill the company's interests and are characterized by effectiveness, transparency and consistency;
- prudence, thoroughness and objectivity in selecting, identifying or hiring and continuing relations with third parties, and in determining the conditions of the relationship for the purpose of preventing the risk of establishing contact with individuals belonging to criminal organizations of any type, whether national or transnational;

- refusal of any consideration in the form of money or other benefit offered by anyone to carry out an act pertaining to his/her job or contrary to his/her official duties;
- compliance with the law, with the requirements issued by the competent Authorities and/or with the internal procedures to delegate spending powers;
- absolute fairness, transparency and thoroughness in accounting entries and tax requirements and in the checks that are a prerequisite for them.

As regards the aforementioned general principles, it is particularly forbidden to:

- establish relations with individuals, entities, companies or associations of any kind established in Italy or abroad, which are known or believed or suspected to belong to, be connected with or have relations of any kind with criminal organizations or groups, or whose identity and fairness has not been thoroughly and diligently ascertained in a traceable manner or documented, and in the case of companies, their actual ownership or relationships of control;
- establish relations with individuals who refuse or are reticent to provide significant information for the purpose of making it known in a fair, real and complete manner, or for which there are suspicious elements also due to having taken place in uncooperative countries, or that request or offer services that may appear to be advantageous for the Company but have suspicious or irregular profiles, or that conduct themselves in a manner that is contrary to the fiscal and accounting laws and regulations governing the circulation of capital and goods;
- bring into the company weapons or substances that are harmful and hazardous to health and safety, such as drugs.

Notwithstanding the general principles of the internal control system in item 2 of the Appendix, and the specific principles described up to now, it is required that the prevention protocols established in this Model are applied to processes that are sensitive to the risk of organized crimes, with reference to the crimes provided for in the Decree.

It follows that, with reference to the sensitive areas at risk of the afore-mentioned crimes being committed, the prevention protocols set forth in the Special Sections for the crimes specified therein constitute an effective preventive measure, also for the crimes of criminal organizations.

6. ACTIVITIES OF THE SUPERVISORY COMMITTEE

The Committee is responsible for:

- periodically checking - with the assistance of the other authorized departments - the validity of the required standard clauses whose purpose is to:
  - ensure that external collaborators and partners comply with the Model and the Code of Ethics;
  - enable FATA to effectively run checks on the recipients of the Model in order to make sure that its provisions are being complied with;
  - implement sanctioning mechanisms (in the case of withdrawal from contract by Partners or external Collaborators, for example) if the requirements are not fulfilled;

- verifying the fulfillment, implementation and suitability of the Model for the purpose of preventing criminal conspiracies;
- issuing and updating standard instructions for the managers of company departments involved in sensitive activities, on how to fill out the following documents in a uniform and consistent manner:
  - forms to periodically notify the Committee as to events that pose a crime risk;
  - evidence sheets to trace activities in contact with the P.A.

These instructions shall be written and kept on paper or electronic media;

- verifying the fulfillment of procedural protocols with particular reference to personnel management, relations with external and intergroup individuals, and accounting and tax requirements;
- evaluating important information sent by the Company.

7. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

Each fact or element that carries a risk of criminal interference/infiltration in company business, with reference to organized crime, must be immediately reported to the Committee by the Recipients (and to their superiors and the competent Authorities), within the timeframe and manner indicated in par. 4.7 "Reporting obligations to the Committee" of this Model.

As a systematic measure to prevent organized crime, the Department Heads must also send the Committee, according to the timeframe and procedures described in this Model and in company procedures, periodical reporting flows concerning the processes that concern them, which fall within the scope of risk stated above.

SPECIAL SECTION "G"

Areas of business in which environmental crimes could be committed, pursuant to article 25 *undecies* of Legislative Decree 231/2001

1. PURPOSE

Special Section G aims to regulate the conduct of Model Recipients, as better defined in the General Section, who are involved in activities where one of the environmental crimes that are considered predicate offences as per art. 25 *undecies* of the Decree and detailed below, could be committed.

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

The rules and principles of conduct set forth in this Special Section constitute an extract of a broader set of internal policies found in the "Integrated Management System for Health, Safety and the Environment" that FATA has developed and implemented, obtaining ISO 14001 certification in March of 2011.

2. TYPES OF CRIMES

With Legislative Decree 121/2011, the legislature intended to extend, by introducing article 25 *undecies* (environmental crimes), the administrative liability of the entity specified in the Decree to include the various types of "environmental crimes", as already required in Directive 2008/99/CE[14] and Directive 2009/123/CE. This Decree modified the penal code, introducing articles 727 *bis* and 733 *bis*, and transposed some of the cases regulated by Legislative Decrees 152/2006 and 202/2007, and by Laws 150/1992 and 549/1993, stating that the entity is liable in the case of conduct that is extremely dangerous for the environment, and that if the responsibility for the illegal act can be attributed to the directors or representatives of legal entities, they shall be jointly liable in accordance with the Decree.

In detail, the new predicate crimes are:

- killing, destruction, capture, collection or possession of wild or protected animal and plant species (art. 727 *bis* of the penal code);
- habitat damage (art. 733 *bis* of the penal code);
- discharge of sewage and collection, handling, shipping, recycling and disposal of waste, including hazardous waste, without the required authorizations, including the monitoring of these operations and inspection of disposal sites, as well as the activity of dealers or brokers; failure to reclaim polluted areas; violation of the limits on atmospheric emissions (Legislative Decree 152/2006);
- import, export, sale, transport, including on behalf of third parties, possession of endangered animal and plant species (Law 150/1992);
- violation of the regulations governing the production, consumption, import, export, possession, collection, recycling or marketing of stratospheric ozone depleting substances and of substances that are harmful to the environment (Law 549/1993);
- intentional and unintentional sea pollution (Legislative Decree 202/2007).

[14] Directive 2008/99/CE forces member states to provide for criminal sanctions in their national body of laws, for serious violations of the provisions of community law on environmental protection. In particular, member states shall ensure that legal entities can be declared liable for the environmental crimes set forth in the Directive if said crimes are committed to their advantage.

3. SENSITIVE PROCESSES

This Special Section refers to conduct by all individuals operating at HQ or on jobsites in Italy and abroad, company representatives, employees, collaborators and consultants of the Company, who are nationally and/or transnationally involved in the following types of company activities:

- office work;
- plant management;
- catering services;
- general services.

To these we can add the following elements that can interact with the environment, thereby constituting possible risks:

- waste generation;
- use of energy;
- water consumption;
- risk of fire and explosion;
- atmospheric emissions;
- use of soil - subsoil;
- presence of asbestos;
- noise emanating outwards;
- presence of underground tanks;
- use of ozone-depleting substances;
- use of carcinogens / mutagens;
- paper consumption.

Sensitive processes also include all the job management activities, design, engineering, procurement, work supervision, manufacture and startup of processing lines for aluminum strip and sheet, and other metals, plants for the production and rolling of aluminum, and plants to generate electrical energy.

The processes described above, which are at risk of environmental crimes being committed as described in this Special Section, may also give rise to the same types of crimes being committed by criminal organizations. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

4. RECIPIENTS OF THIS SPECIAL SECTION

The Recipients of this Special Section are the Directors, General Managers (top management figures) and Statutory Auditors of the Company, as well as the employees subject to surveillance and control by management individuals in at-risk business areas, hereinafter referred to as "**Recipients**".

As regards the Directors, General Directors and Statutory Auditors, the law equates those who perform these duties "de facto" with those who are formally vested with these titles. Pursuant to art. 2639 of the civil code, in fact, anyone who performs the same job that is described differently, as well as anyone who continuously exercises the typical powers of the title or job must answer for environmental crimes.

The aim of this Special Section is to ensure that all the Recipients are fully aware of the significance of censurable conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

5. GENERAL RULES OF CONDUCT

This chapter describes the rules of conduct to be adopted by company representatives, consultants and commercial partners and third parties.

This chapter aims to ensure that these individuals, to the extent that they are involved in the activities belonging to the so-called at-risk areas, and in consideration of their different positions and obligations with respect to the company, abide by the rules of conduct established herein to prevent environmental crimes from being committed.

Consequently, in performing their duties, the Directors, Auditors and employees shall comply with the rules of conduct indicated below.

General Rules of Conduct

- Establish company policy as regards health, safety and protection of the environment;
- carry out activities in accordance with the principles set forth in the Code of Ethics, Organizational Model, company policies and Directives of the Parent Company;
- refrain from engaging in conduct that, even if it does not actually constitute one of the crimes considered above, could potentially become one;
- conduct yourself in a fair and transparent manner in full compliance with the laws and regulations and with internal company procedures;
- follow the rules in the manual of integrated management system for health, safety and the environment, in the related procedures, work instructions and operating documents;
- maintain a working performance monitoring and measurement system in order to keep ISO 14001 certification;
- establish the procedures and responsibilities for access, identification, keeping, diffusion and updating of legal and other requirements concerning the environment;
- establish the responsibilities and procedures to properly disseminate information concerning environmental impacts;
- report environmental situations that require special attention.

Requirements and Skills

- Formal identification of roles and associated responsibilities;
- determining at-risk areas and the tasks carried out in each of these areas;
- identification of individuals to ensure that maintenance-improvement measures are being implemented.

Education and Training

- Raising awareness on the importance of the environmental management system and on one's role in order to implement environmental policy;
- training necessary to acquire specific skills upon recruitment in the case of job change or new activities;
- evaluating training requirements and degree of effectiveness.

Registers and Other Documents

- Keeping a log of environmental obligations.
- keeping a log on the level of education, training and experience of personnel;
- keeping a record of risk assessment activities by area and task, indicating the instruments and methods used to make the assessment and the schedule of measures to maintain and improve them;

- requesting and assessing the safety and coordination plans (PSC) issued for the various jobsites.

6. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The Department Head is responsible for periodically bringing the following to the attention of the Committee:

- List of principal obligations regarding:
  - proper issuing of required environmental authorizations or certificates;
  - monitoring and updating of the initial environmental analysis;
  - periodical review of ISO 14001 certification, indicating the suggested corrective actions;
  - waste management.

- any checks or inspections - either internal or external - complete with results, on any requested work and any sanctions applied to the Company.

SPECIAL SECTION "H"

Areas of business in which smuggling crimes could be committed, pursuant to article 25 *sexiesdecies* of Legislative Decree 231/2001

1. PURPOSE

Special Section H deals with smuggling crimes and refers to the cases of conduct indicated in Art.25-*sexiesdecies* of the Decree.

The aim of this regulation is to ensure that all the people involved conduct themselves in accordance with the Model in order to prevent the smuggling crimes under Art.25 *sexiesdecies* from being committed.

2. SENSITIVE PROCESSES

The corporate activity to be considered for the purpose of preventing the predicate crimes in question is:

- Management of customs obligations

The processes described above, which are at risk of smuggling crimes being committed as described in this Special Section, may also give rise to the same types of crimes being committed by criminal organizations. It follows that the prevention and control protocols indicated below are also a way to prevent criminal conspiracy, in addition to the specific general principles in Special Section F.

3. RECIPIENTS

This section of the Model is intended for company individuals (the "**Recipients**") who, because of their position, role or corporate function, are required to apply or comply with it, in the performance of at-risk activities.

The aim of this Special Section is to ensure that all the Recipients are aware of the significance of their conduct and adopt the rules of conduct described herein, in order to prevent the crimes listed in the Decree from being committed.

4. GENERAL RULES

The system in general

The aim of this Section is to ensure that anyone who is involved in activities where one of the specified crimes could be committed abide by the rules of conduct described herein for the purpose of preventing conduct that could directly or indirectly lead to smuggling crimes.

In particular, when performing these activities it is strictly prohibited to create, collaborate or give rise to types of conduct that taken individually or collectively, could directly or indirectly lead to crimes related to non-cash payment instruments.

Specific procedures and instructions

When performing operations that are pertinent to at-risk activities, in addition to the rules of the Model, the Recipients of this prevention system must comply with:

- applicable Italian and foreign legislation;
- Code of Ethics;
- internal control system (principles of *corporate governance*, company procedures and guidelines, documentation and provisions on organizational structure and management control system approved by the Board of Directors);
- regulations governing the administrative, accounting, financial and *reporting* systems of the Company;

– applicable laws, standards and regulations of market regulatory authorities (CONSOB and the Italian Stock Exchange in particular).

General Rules of Conduct

Anyone involved in dealing with customs obligations is strictly prohibited from implementing or giving rise to conduct that could directly or indirectly lead to crimes involving non-cash smuggling.

The different positions and obligations of each individual are taken into consideration for sanctioning purposes.

Consequently, the company expressly requires that:

- roles and responsibilities be decided and assigned to properly manage customs procedures;
- import operations be run by skilled and properly trained personnel;
- the goods be monitored to ensure they are properly classified (TARIC);
- the selected forwarding agents be registered and known nationally and/or internationally;
- relations with forwarding agents be formalized in a contract;

the value declared at customs is correct.

5. ACTIVITIES OF THE SUPERVISORY COMMITTEE

The Committee shall verify the existence, the actual compliance with the real situation and the precise application of the items given below as examples:

- any inspections and/or checks performed by the Customs Agency.

6. INFORMATION FLOWS TO THE SUPERVISORY COMMITTEE

The heads of the departments in question shall on a regular set basis inform the Committee of all abnormal situations and conduct that concern them, observed by anyone, and the transactions performed departing from the above-mentioned principles, with reference to the specific company processes that are at risk of a crime being committed, and together with the periodical flows indicated in Special Section A.

APPENDIX

1. DIRECT TRANSACTIONS BY TOP MANAGEMENT FIGURES "THAT DO NOT FOLLOW PROCEDURE"

FRAME OF REFERENCE

According to art. 5 of the Decree, top management figures are defined as "*people occupying positions of representation, administration or management of the Entity or one of its financially and operationally independent subsidiaries, and people exercising de facto management and control of the company*".

The Decree has not modified the system that regulates the running and governance of companies, so the decision-making independence of top management figures is a substantial and unwavering expression of freedom of management of corporations.

Top management figures ordinarily decide to carry out transactions that follow the criteria in the Model, of which they are aware and with which they are in agreement. However, these individuals are at times required - in the company's interest - to enter into transactions that follow a procedure other than the one specified in the Model, due to exceptional situations of extraordinary urgency or particular situations of confidentiality or even because of the particular nature of the transaction.

This internal control system refers to this last type of transaction.

CONTROL ACTIVITIES

The control system is based on two key elements, i.e. **document traceability** and **flow of information** to the Committee.

Listed below are the specific control elements:

- Transaction traceability in terms of documentation and electronic media that allow the subsequent "reconstruction" of the reasons and contingent situations in which the transaction occurred. Special consideration must be given to the explanation, still in summary form (but not general), of the reasons and causes that led to the choice. The reasons for the decision do not necessarily have to be explained, but rather the characteristics (i.e. confidentiality and urgency) that made it impossible to make the decision according to the established procedures;
- Specific information provided to the Committee by the top management figure who "exceptionally" initiated the transaction, allowing the Committee to respond systematically and promptly. It is also important to emphasize that another element that can strengthen the system is the "capture" of transactions of "top management figures" through information flows concerning "exceptional" transactions, as per the individual internal control system on instrumental processes. These flows, in fact, contain details on "exceptional" transactions (regardless of where they originated) sent to the Committee by the managers of the departments that actually carried them out.

2. GENERAL PRINCIPLES OF INTERNAL CONTROL

The "**internal control system**" contains all the "instruments" used for the purpose of providing reasonable assurance that targets will be reached relating to operating efficiency and effectiveness, reliability of financial and operating information, compliance with laws and regulations, and safeguarding of assets against possible fraud.

The internal control system is characterized by general principles whose scope of application is continuously extended through the various organizational levels (*Business Unit*, Department, hereinafter "**Organizational Unit**").

General control environment

Responsibilities have to be determined and duly distributed without overlapping or assigning operating responsibilities that concentrate critical activities in a single individual.

No significant transaction (in terms of quality and quantity) for the Organizational Unit can originate or be initiated without authorization.

Powers of representation shall be conferred according to operating areas and set amounts that are strictly tied to the assigned tasks and organizational structure.

The operating systems shall be consistent with company policy and the Code of Ethics. In particular, the company's financial information shall be prepared:

- in compliance with laws and regulations;
- in compliance with the established accounting standards;
- consistently with the established administrative procedures;
- within the scope of a complete and updated chart of accounts.

Risk Assessment

The targets of the Organizational Unit shall be established and made known to all the levels concerned for the purpose of clarifying and sharing them.

The risks related to reaching the targets shall be identified, periodically monitored and updated.

Negative events that can threaten operating continuity shall be subject to risk assessment and updating of protective mechanisms.

Control Activities

No one person shall have full control of an entire process/activity; a suitable role separation procedure shall be established.

The operating processes shall have a suitable documentary / system support so that their accuracy, consistency and responsibility can be continuously verified.

Operating choices must be traceable in terms of characteristics and reasons, and it must be possible to identify those who authorized, carried out and verified each activity.

Mechanisms have to be provided to ensure the entirety and completeness of handled data with respect to the exchange of information between consecutive phases/processes.

Information and Communication

A system of indicators according to process/activity has to be set up together with a periodical *reporting* flow to *management*.

Administrative and managerial Information Systems shall be oriented towards integration and standardization.

Safety mechanisms shall ensure protection / physical-logical access to data and assets of each Organizational Unit.

Monitoring

The control system is subject to continuous monitoring and periodical assessment so it can be constantly updated.

3. PRINCIPLES OF CONDUCT WITH THE P.A.

This document contains the conduct guidelines the Company must follow to prevent the creation of any situations that are conducive to the perpetration of the crimes set forth in the Decree.

The guidelines refer to "positive behaviors" and "negative behaviors" specifying in operational terms what is expressed in the principles of the Code of Ethics.

POSITIVE BEHAVIORS

- Department heads who have business contacts with the P.A. shall:
  - provide their collaborators with directives regarding the type of conduct to adopt in formal and informal dealings with various public officials, depending on the characteristics of their business, by transferring knowledge of the rules and awareness of the situations in which there is a risk of a crime being committed;
  - set up suitable mechanisms to trace the information flows to the P.A.

- Assigning external individuals to represent FATA in its dealings with the P.A. shall be done formally, and a specific clause shall be included that binds the parties to comply with the ethical-behavioral principles adopted by the Company.
- Employees and external collaborators are requested to report to the Committee any violation or suspected violation of the Model. The reports can only be provided non-anonymously.
- The Company and the Committee will safeguard employees and external collaborators against any harmful effect resulting from the report.
- The Committee ensures that the identity of the individuals who submit a report will remain confidential, notwithstanding the obligations of the law.
- The department heads shall report to the Committee any behaviors in their operating processes that constitute a crime risk under the Decree, of which they became aware directly or through a report received from one of their collaborators.
- In particular, in the case of attempted blackmail of an employee (or other collaborator) by a public official, the following conduct shall be adopted:
  - do not act on the request;
  - immediately inform your superior;
  - the superior must then make a formal report to the Committee.

- The department heads who officially learn of news, including from the judicial investigative police, concerning wrongdoings and/or crimes that carry the risk of impacting the company, shall report it to the Committee.

NEGATIVE BEHAVIORS

With reference to the types of crimes envisaged in the Decree, a non-exhaustive list of at-risk behaviors to be avoided is given below.

In dealing with representatives of the P.A., it is forbidden to:

- promote or make monetary payments for purposes other than institutional or service-related ones;
- promise or grant "privileged solutions" (i.e. facilitating the hiring of relatives / in-laws / friends, etc.);
- spend money on unjustified entertainment expenses for purposes other than the mere promotion of the company's image;
- promise to supply or wrongly supply, including through third parties, works / services (i.e. restructuring of private residential buildings, etc.);
- promise or grant gifts / gratuities, either directly or indirectly, of significant value;
- provide or promise to provide confidential information and/or documents;
- in acquisitions, favor suppliers or subsuppliers indicated by the representatives themselves as a condition for the activity to take place (i.e. job awarding, granting of subsidized loans).

The above prohibitions also cover indirect relations with the P.A. officials through trusted third parties.

Moreover, when dealing with the P.A., it is forbidden to:

- show false or forged documents / data;
- behave deceptively in order to mislead the P.A. as to the technical and economic assessment of the products and services being offered/supplied;
- omit required information for the purpose of steering the P.A. towards making decisions in one's favor;
- allocate contributions / subsidies / public loans for purposes other than those for which they were granted;
- access the P.A. information systems without authorization to obtain and/or change information to the advantage of the company;
- abuse one's position as manager / maintenance technician of the P.A.'s ICT systems for the purpose of obtaining and/or changing information to the advantage of the Company.

4. COMPATIBLE PUBLIC ENTITIES ACCORDING TO LEGISLATIVE DECREE 231/2001

- The administrative offices of the P.A., including all types and degrees of institutes and schools, educational institutions and universities;
- Autonomous state companies and administrative offices;
- Regions, Provinces, Municipalities, Mountain Communities and their consortiums and associations;
- Autonomous institutes for public housing;
- Chambers of Commerce, Industry, Craftsmanship and Agriculture;
- National, regional and local non-economic public entities;
- Administrative departments, companies and entities of the National Health System;
- Public service concessions authorities, public officials and public service officers;
- Members of the Commission of the European Union, the European Parliament, the Court of Justice and the Court of Auditors of the European Union;
- Officials and agents contracted according to the staff regulations of officials of the European Union;
- People ordered by Member States or by any other public or private entity in the European Union to perform functions that are equivalent to those of the officials or agents of the European Union;
- Members or agents of entities based on the founding treaty of the European Union;
- Those who perform functions or activities equivalent to those of public officials or public service officers for the other Member States of the European Union;

– Those who perform functions or activities equivalent to those of public officials and public service officers for foreign countries that do not belong to the European Union or for international public organizations.